



### 2008 AICPA Information Technology Conference

Protecting Information Outside of the Firm:  
Mobile Data & Device Security  
Eric McMillen CISSP, CISM, CISA  
June 9, 2008



---

---

---

---

---

---

---

---

### Session Objectives

- Discuss the security and privacy issues involving data on laptops and mobile devices.
- Present you with potential risk mitigation options



---

---

---

---

---

---

---

---

### The Problem

- May 2005, laptops accounted for 53.3% of the total PC retail market.
- A laptop is stolen every 53 seconds. 90% are never recovered.
- 73% of companies had no specific security policies for their laptops in 2003.
- 42 States have enacted Data Breach Laws since 2003
- "The loss or theft of just one laptop can cost a company as much as \$90,000 or more in fines, credit monitoring for victims, public relations damage control, and class action litigation." Robert Siciliano, Identity Theft Expert



---

---

---

---

---

---

---

---

### 4 Phases of Mobile Data Security

- Planning
- Protection
- Response
- Recovery



---

---

---

---

---

---

---

### Planning Phase

- Understand your business
- Develop a Data Classification Policy
- Perform a Mobile Asset Risk Assessment
- Develop a Mobile Data/Computing Policy



---

---

---

---

---

---

---

### Understand Your Business

- Compliance requirements and regulations
  - PCI
  - GLBA
  - FFIEC
  - SOX
  - State statutes
- Where does your data reside?
- What mobile data is necessary vs. convenient



---

---

---

---

---

---

---

## 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. Address (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



---

---

---

---

---

---

---

---

## Data Classification

- Not All Data is Created Equal
- Minimum of Four Classifications
  - Public – Intended for the distribution to and viewing by the general public.
  - Confidential – For use by staff, contractors, and business partners only.
  - Proprietary – Intellectual property of the firm.
  - Secret – For use only by designated individuals with a need to know.



---

---

---

---

---

---

---

---

## Risk Assessment Process

- Identify information assets
- Identify threats for each asset based on C.I.A.
  - Confidentiality-prevent unauthorized disclosure
  - Integrity-ensure accuracy and authenticity
  - Availability-ensure that information and systems are there when you need them
- Identify controls to protect your assets from these threats



---

---

---

---

---

---

---

---

### Risk Assessment Process Cont'd

- Key Questions during the Risk Assessment Process
  - What could happen?
  - If it happened, how bad could it be?
  - What can be done to prevent it from happening?
  - How much will it cost?
  - Is it cost-effective?



---

---

---

---

---

---

---

---

### Establish a Mobile Data/Computing Policy

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



---

---

---

---

---

---

---

---

### Protection Phase

- Defense in depth
- Essential Aspects to Protect Mobile Data
  - Physical Security
  - Authentication
  - Secure Configuration
  - Encryption
  - Backups
  - Education



---

---

---

---

---

---

---

---

### Physical Security

- Easiest to implement - Most often ignored.
- Basic Physical Security Guidelines
  - Don't take data out of the office unnecessarily.
  - Maintain positive control of your laptop.
  - Use privacy screens to help prevent shoulder surfing.
  - Utilize laptop locking cables and/or alarms.
  - Keep laptops out of sight when not in use.
  - 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 - password
  - Something You Have – token or certificate
  - Something You Are - biometrics
- The problem with passwords
- Two-factor authentication
  - Security tokens
  - Smart-cards & certificates
  - Biometrics



---

---

---

---

---

---

---

---

### Secure Configuration

- Develop and use a Hardening Checklist
- Basic steps to take
  - Application and OS updates
  - Disable wireless interfaces (When not in use)
  - Personal firewall – software or hardware
  - Updated anti-malware software
  - Locking screensavers
  - Restrict Administrative access
  - Restrict mass storage devices to only those authorized



---

---

---

---

---

---

---

---

### Encryption

- Whole Disk Encryption vs. Targeted Encryption
- Encryption Issues
  - Cipher Strength
  - Key Management
  - Bad Pass Phases
  - Performance
- Product Types
  - Hardware -
  - Built-in to the operating system
  - Third-party software



---

---

---

---

---

---

---

---

### Backup

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



---

---

---

---

---

---

---

---

### Education

- Using it is different than 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

- Incident Response Planning
- Breach Notification



---

---

---

---

---

---

---

### 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 must be notified
- Timing of a breach notice
  - In general, notify as soon as reasonably possible
  - Possible delays for law enforcement investigations
- Required Channels for communicating



---

---

---

---

---

---

---

**AICPA** conferences

### Recovery

- Goals of Recovery
  - Recover lost or stolen mobile data
  - Return lost or stolen devices to the control of the firm
- Laptop Tracking Technology
- When Recovery is not possible

AICPA

---

---

---

---

---

---

---

**AICPA** conferences

### Tracking Technology

- Benefits
  - Reduce Internal Theft
  - Relatively Low Cost
- Tracking Myths
  - Thief will connect to the Internet right away
  - High Recovery Rate

AICPA

---

---

---

---

---

---

---

**AICPA** conferences

### “Poison Pill” Technology

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

AICPA

---

---

---

---

---

---

---

### Your Action Plan

- > Inventory and classify your firm's data
- > Perform a risk assessment
- > Develop or revise your mobile computing/data policy
- > Implement your controls based upon your policy and risk assessment
- > Educate all of your staff on your policy and their responsibilities
- > Develop and practice your incident response plan



---

---

---

---

---

---

---

---

# Questions??



---

---

---

---

---

---

---

---

# Thank You!

Eric McMillen, CISSP CISM CISA  
The McMillen Group, LLC  
<http://www.mcmillengroup.com>  
[emcmillen@mcmillengroup.com](mailto:emcmillen@mcmillengroup.com)  
Phone: 214.329.9730  
Fax: 866.375.6006



---

---

---

---

---

---

---

---

## PORTABLE COMPUTING SECURITY POLICY

### **PURPOSE:**

The purpose of the Portable Computing Security Policy is to establish safeguards for the use of portable media and computing devices, including their connection to the Firm's network.

### **SCOPE:**

Portable computing devices are becoming increasingly powerful and affordable. With the growing need for instant communication and data access, the use of portable computing devices is becoming ever more desirable to replace traditional desktop devices in a wide number of applications.

This policy applies to anyone who utilizes portable computing devices to access the Firm's information and computing environment, including Firm owned, personally owned, or third-party owned portable computing devices.

This policy is not intended to address the use of portable computing devices by the general public to access the Firm's electronic data and services.

### **POLICY:**

The Firm shall determine whether it will permit the use of both privately owned and company-owned portable computing devices and the level at which the devices are maintained and managed.

### **DEFINITIONS:**

- **Portable computing devices** - These include, but are not limited to, Portable Digital Assistants (PDAs), notebook computers, Tablet PCs, Palm Pilots, Microsoft Pocket PCs, RIM Blackberrys, MP3 players, text pagers, smart phones, and other similar devices.
- **Portable media** - This includes, but is not limited to, compact disks, DVD disks, memory sticks, USB drives, floppy disks, etc. The portability offered by these devices may increase the risk of exposure to groups using the devices.
- **User** - Anyone with authorized access to the the Firm business information systems, including permanent and temporary employees or third-party personnel such as temporaries, contractors, consultants, and other parties with valid the Firm access accounts.
- **Firewall** – Software, or a combination of hardware and software, that implements security policy governing traffic between two or more networks or network segments. Used to protect internal networks, servers, and workstations from unauthorized users or processes. Firewalls have various configurations, from stand-alone servers to software on a laptop computer, and must be configured properly to enable protection.
- **Screen Locking** - Mechanism to hide data on a visual display while the computer continues to operate. A screen lock requires authentication to access the data. Screen locks can be activated manually or in response to rules.
- **Screen Timeout** - Mechanism to turn off a device or end a session when the device has not been used for a specified time period.

## PROCEDURES:

### Section 1 Physical Security

Users must protect the Firm-owned (or authorized) portable computing devices, removable storage components, and removable computer media from unauthorized access. Physical security measures shall, at a minimum, include the following:

- Portable computing devices, computer media, and removable components, such as disk drives and network cards, must be stored in a secure environment. Devices must not be left unattended without employing adequate safeguards such as cable locks, restricted access environments, or lockable cabinets.
- When possible, portable computing devices, computer media, and removable components must remain under visual control while traveling. If visual control cannot be maintained, then necessary safeguards shall be employed to protect the physical device, computer media, and removable components.
- Safeguards shall be taken to avoid unauthorized viewing of sensitive or confidential data in public or common areas.

### Section 2 Operation and Maintenance

The Firm has established minimum portable computing device configuration requirements for company-owned, privately owned, or contractor-owned devices authorized for work use. The requirements must identify who is authorized to prepare portable devices for use on the Firm Business Information Systems, network, or telecommunications systems. The configuration guidelines address the following:

- **Anti-virus software:** Portable computing devices must be equipped with anti-virus software in accordance with the the Firm User Malicious Software Policy.
- **System configuration:** Mandatory system configurations, settings, and software for either company-owned or authorized non-company-owned devices must not be modified without prior authorization by the Security Administrator. Portable computing device operating systems must be maintained with appropriate vendor security patches and updates.

### Section 3 Data Protections

Given their small size and portable nature, it is more likely that these portable computing devices will fall into the wrong hands than a desktop system. The following guidelines are used to govern the management and maintenance of personal and company data on portable computing devices:

- Sensitive the Firm data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive the Firm data stored on portable computing devices must be secured in accordance with the Firm's data encryption policy.
- All portable computing devices used to access the Firm's data must follow the appropriate methods for securing the system. Methods for securing portable computing devices include, but are not limited to:
  - Personal Firewalls;
  - BIOS Passwords;
  - Screen Locking;
  - Screen Timeout;
  - Security Tokens.
- The Firm data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized.

- If sensitive data is transferred/synchronized either via wire (LAN/WAN or Public Internet) or wireless connections (including to and from web sites, server databases, or email servers), it must be transmitted in an encrypted format using the the Firm's centralized, secured server. Using alternative methods of synchronization including PC/MAC based synchronization software included with the portable computing devices to synchronize with the Firm sensitive data sources is prohibited and subject to progressive discipline up to and including termination.
- Use of the included synchronization software from the portable computing devices manufacturer is permitted when the data sources are not considered sensitive under the Business Systems Management Control Framework policy.
- Portable computing devices must not be equipped with remote system or application administrator privileges unless authorized. Portable computing devices equipped with remote system administrator capabilities must be assigned higher levels of security in accordance with the increased risk of an IT security breach or loss of device pursuant to the Business Systems Management Control Framework Policy.
- All remote access (dial in services) to the Firm must be either through an approved modem pool or via an Internet Service Provider (ISP). Refer to the Remote Access Policy for more information.
- Real time access to sensitive data using internal or public wireless networks requires the installation of the Firm's Virtual Private Network (VPN) software on the portable computing devices. This software will provide for the requisite strong authentication and continuous encryption of the data.
- There are policies and procedures for the return of the Firm-owned portable computing devices when the user's employment or contract terminates, or the user's assignment no longer requires the company-owned device. Such policies and procedures will include whether non-company data and software are permitted and if so, who is responsible for their removal.
- When a device is removed from service, the IT equipment must be sanitized to remove information.
- The Firm must ensure that all company data and software are recovered, deleted, and securely overwritten as appropriate from privately owned and contractor-owned portable computing devices when the user's employment or contract terminates, or when the portable computing device is no longer authorized for work use.

#### **Section 4      Inventory and Audit**

The Firm must develop and maintain an inventory for all company owned, privately owned, and contractor-owned portable devices authorized for work use with the Firm's Business Information Systems. The inventory shall include the device make, model, serial number, date introduced into service, and party responsible for the device.

Inventory and security audits of portable computing devices are conducted and documented on both a regular and random basis.

#### **Section 5      Enforcement**

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or legal action as appropriate, or both.

## **Section 6      Policy Update and Notification**

the Firm reserves the right to revise the conditions of this policy at any time by giving notice via the Information Security Policy Update Procedure. Users are responsible for understanding or seeking clarification of any rules outlined in this document and for familiarizing themselves with the most current version of this policy.

## **Section 7      Related Documents**

- Business Systems Management Control Framework Policy
- Information Security Policy Update Procedure
- Remote Access Policy
- User Malicious Software Policy

## 2008 AICPA Information Technology Conference

### Protecting Information Outside of the Firm - Resources

#### Data Breach Information

Security Breach Notification: State Laws Chart -

<http://www.perkinscoie.com/files/upload/securitybreach.pdf>

FTC Identity Theft - <http://www.ftc.gov/bcp/edu/microsites/idtheft/business/index.html>

Privacy Law Blog - <http://privacylaw.proskauer.com/>

#### Two Factor Authentication Products

SecuriKey - <http://www.securikey.com/>

PointSec - <http://www.pointsec.com>

#### Hardening Checklists

NIST - <http://csrc.nist.gov/checklists/>

Center for Internet Security - <http://www.cisecurity.org/>

NSA - <http://www.nsa.gov/SNAC/>

Microsoft - <http://www.microsoft.com/technet/security/default.msp>

#### Mobile Hardware Firewalls

Yoggie Gatekeeper Pro - <http://www.yoggie.com/>

#### Encryption Products

PGP - <http://www.pgp.com>

Credant Mobile Guardian - <http://www.credant.com/>

PointSec Media Encryption - <http://www.pointsec.com/>

Full Disk Encryption Wiki - [http://www.full-disk-encryption.net/wiki/index.php/Main\\_Page](http://www.full-disk-encryption.net/wiki/index.php/Main_Page)

#### Tracking Products

CyberAngel - <http://www.sentryinc.com/>

CompuTracePlus - <http://www.absolute.com/>

# Selecting A Password

One of the easiest ways for a person to crack a computer system is by gaining a toehold via a user's personal account. This is frequently possible when accounts have easily guessed passwords (e.g., when the password is the same as the username or the person's first or last name, etc.) Studies have shown an alarmingly high percentage of insecure passwords on typical systems, in the range of 30 to 70%.

Computer hackers use very sophisticated techniques to determine your password so they may break into your account and attempt to gain control of other computer resources or accounts on the computer system. Because of these techniques, it is difficult to create a completely unbreakable, secure password.

The following recommendations will help you select a secure password. Please incorporate these recommendations; they discourage hackers, and assist us in protecting the firm's computing resources. Remember, if you do not select a good password, someone could use your account and breach our security system, jeopardizing other computer users and accounts.

**Periodic Expiration.** Passwords expire on a regular basis. When you log in, if you see a message indicating that your password will expire, change it immediately. If you do not, you will be completely locked out of the network.

**Guessed Passwords.** A password-cracking program should be run periodically by the IT Department on all network systems to locate any accounts with easily guessed passwords. Warning mail is sent to the accounts, and their passwords are expired. This will force a password change at the next login.

## Selecting a "Good" Password

There are 8 main principles in the selection of a good password:

1. Do not use words or word combinations that can be found in any dictionary, in *any* language. Cracking programs found on the Internet can easily break these types of passwords.
2. Be sure your password is at least 7 characters long, 10 or more is better. The longer your password is, the longer it will take a hacker or cracking program to try figure it out. Adding a few characters to your password could add days or weeks to the time it would take to crack it, thus discouraging many would-be hackers. Windows passwords should be either 7 or 14+ characters long, due to the way that the operating system stores the corresponding LanMan hashes.

3. Try to use upper and lower case letters. Many passwords are *case sensitive* which basically means that upper and lower case letters are not considered the same. For example, "N" is not the same as "n" in a password.
4. Using numbers in your password also makes it more difficult to guess.
5. It is also a good idea to have at least one symbolic character in your password. Examples of symbolic characters are: &, \$, \*, ', #, @, etc. . .
6. Don't use personal information such as your phone number, birthday, cat's name, or mother's name.
7. Use a *different* password for each of your computer accounts.
8. Select a password that is easy for *you* to remember but difficult for anyone else to guess.

To select a password you can easily remember, follow these tips:

- Combine several words together and form a phrase that is not in any dictionary. For example, using the previous suggestions, combine the words ate, my, and hat to form the password *8my\$Hat*.
- Take a favorite phrase or song lyric and creates a password using the first or last letter of each word. For example, It is a very fine day could be abbreviated to iiavfd, and then by adding two non-alphabetic characters, would become a valid password of *iia44fd*.
- Choose a word, and then scramble it with some random numbers (e.g., buffalo becomes *Bu3fa2o*).

Here are some examples of good and bad passwords:

- *g2so98oners* is a good password. *goso98oners* is not.
- *o8at45s* is a good password. *oats22* is not.