



ANAHEIM
2009

The Annual Conference of the Financial Planning Community

TRACK:	<i>PRACTICE MANAGEMENT & TECHNOLOGY</i>
SESSION: 979035	SECURING INFORMATION AMIDST THE REGULATORY LANDSCAPE
	MONDAY, OCTOBER 12, 2009
	8:15 AM - 9:30 AM
PRESENTER:	Michael Sundberg
	Commonwealth Financial Network
	29 Sawyer Road
	Waltham, MA 02453

Michael joined Commonwealth in July 2000. In his current role, he serves as the overall program manager for Corporate Information Security. Working with the rest of the Technology team, as well as with the Compliance and Legal departments, he performs systems security assessments, reviews and interprets regulatory regulations, and coordinates and influences projects that strengthen the security posture for Commonwealth, its advisors, and their clients. Previously, Michael worked as the Director of Technology Support and Training for the firm's employees and advisors. During this time he helped to build Commonwealth's support infrastructure, with the mission of providing a superior support experience. Michael graduated from Rhode Island College, earning his bachelor's degree in management, with a concentration in human resource management. He is currently a Certified Information Security Manager candidate.

Securing Information Amidst the Regulatory Landscape

Michael Sundberg
Director of Information Security
Commonwealth Financial Network®

member FINRA/SIPC, a registered investment adviser

The New Normal

- ▶ Regulations
 - GLBA Regulation S-P
 - FTC red flag rules
 - State notification laws
 - Victims must act quickly to minimize the damage

The New Normal *continued*

- State safeguarding laws
 - Differ greatly
 - Slowly starting to resemble some consistency
 - Mass 201 CMR 17.00
- Federal safeguarding laws?

What Is Required?

- ▶ Information security program
 - Appointment of security officer
 - Risk-based approach
 - Reasonable to size organization
 - Ongoing risk assessments
 - Documented policies and procedures
 - Ongoing education
 - Audit effectiveness of policies and program

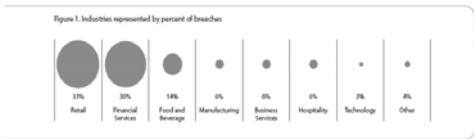
A Few Examples of Doors

- Unencrypted wireless network
- Unencrypted laptop or portable media
- Smash-and-grab break-in
- Shared fax machine
- Rogue employee
- Vendor and third parties
- Virus/keystroke logger
- Social engineering
- Improper disposal of hardware and paper



Number of Breaches by Industry

▶ Retail continues to be the most frequently affected industry claiming 31% of all breaches. **The major gainer in 2008 was financial services, which doubled in terms of caseload percentage to 30 percent.**



Verizon Business 2009 Data Breach Investigations Report

It Happens

- ▶ Bank of New York Mellon
 - vendor mistake—lost unencrypted backup tapes
- ▶ Heartland Payment systems
 - Tens of millions of credit card numbers breached—improperly secured wireless network
- ▶ TJX
 - 94 million credit card numbers exposed—improperly secured wireless network

It Happens *continued*

- ▶ Florida doctor
 - Donated computer to family in need—did not wipe information off computer

Document/CD Shredding Policy for **Company Name**

Last Revision Date: **mm/dd/yyyy**

1.0 Purpose

To ensure the proper disposal of paper documents and CDs that may or may not contain sensitive client information, and to protect against unauthorized access to or use of customer records, **Company Name** is implementing a Document/CD Shredding Policy, effective as of the date listed above.

2.0 Scope

This policy applies to the disposal and shredding of all documents and CDs containing sensitive client information.

3.0 Policy

Paper documents and CDs to be recycled should be separated from those to be shredded. Any document or CD containing sensitive client information that is ready for disposal must be shredded in a secure area and discarded to ensure disposal. If an employee is unsure whether or not a document/CD contains sensitive client information, the document/CD should be shredded.

4.0 Please initial the box below to indicate that you have read and understood this policy.

Circulate to	Initial	Date	File Compliance	File Memo Binder

End-of-Day Procedures for **Company Name**

Last Revision Date: **mm/dd/yyyy**

1.0 Purpose

Company Name must follow certain procedures at the end of each workday in order to safeguard all confidential information held within the office. This policy explains what steps must be taken to secure information at the end of each day and is effective as of the date listed above.

2.0 Scope

This policy applies to all employees of the **Company Name** facility.

3.0 Policy

(The following examples may or may not be applicable to your office. Please modify them to suit your office.)

At the end of each workday, the following procedures will occur:

1. All filing cabinets containing confidential information will be locked.
2. Any loose papers containing confidential information will be properly stored away and placed in a safe location.
3. All computers will be locked and/or shut down.
4. Deadbolts will be secured.
5. The alarm system will be activated.
6. The last employee to leave will ensure that all others have left the building before locking up.

4.0 Please initial the box below to indicate that you have read and understood this policy.

Circulate to	Initial	Date	File Compliance	File Memo Binder

Hardware Disposal Policy for **Company Name**

Last Revision Date: mm/dd/yyyy

1.0 Purpose

To ensure the proper disposal of retired hardware and protect sensitive data in accordance with SEC regulation S-P, **Company Name** is implementing a Hardware Disposal Policy, effective as of the date listed above.

2.0 Scope

This policy applies to all hardware ready to be retired. Hardware is defined as hard drives, desktop and laptop computers, servers and storage devices, monitors, printers, and scanners.

3.0 Policy

- A. **Department/person** must ensure that all data stored on hardware is made inaccessible by either removing or destroying it.
- B. Once data elimination is verified, an appropriate recycling method is to be utilized.
 - i. Hardware that still functions can be donated, provided that all data stored on the hardware is made inaccessible.
 - ii. Hardware beyond economical repair must be disposed of by an accredited vendor.
 - a. A certificate of destruction or other meaningful documentation should be presented to ensure that the items have been properly disposed of.

4.0 Please initial the box below to indicate that you have read and understood this policy.

Circulate to	Initial	Date	File Compliance	File Memo Binder

Visitor Policy for **Company Name**

Last Revision Date: **mm/dd/yyyy**

1.0 Purpose

Company Name has implemented identification procedures that increase security for staff and visitors, effective as of the date listed above. These measures allow for the proper identification of visitors entering and working in **Company Name**'s facility. These security procedures have been implemented with respect to the size and dynamic of the **Company Name** facility.

2.0 Scope

This policy applies to all visitors of the **Company Name** facility.

3.0 Policy

- A. All visitors of the **Company Name** facility should provide identification and identify the employee with whom they are meeting.
- B. The appropriate **Company Name** employee who is being visited is expected to escort the visitor in the building at all times of the visit.
 - i. If, due to business circumstances, the visitor cannot be escorted by a **Company Name** employee at all times, the visitor must sign a Confidentiality Agreement.

4.0 Please initial the box below to indicate that you have read and understood this policy.

Circulate to	Initial	Date	File Compliance	File Memo Binder