

Automating Security Administration

Are We There Yet?



A MILLIMAN GLOBAL FIRM

Milliman

Consultants and Actuaries

John Phelan, Ph.D.
HIPAA Summit XIII
September 26, 2006

Session Agenda

- The Problem
- Options
- What is an administrative system?
- Selection criteria
- Case studies
- Are we there yet?



Why Bother

- Regulatory requirements
- It's the right thing to do
- Patient/participant/client/customer concerns
- Legal concerns
- Headlines



Headlines

- **Former Cleveland Clinic worker, kin charged with fraud, HIPAA violation**
- **Subcontractor Notifies VA of Missing Computer with Vet Files: *VA, Law Enforcement Authorities Investigating***
- **MAN PLEADS GUILTY IN ATTACK ON HOSPITAL COMPUTER SYSTEM**
- **Flurry of new data breaches disclosed**
- **Four lose jobs after data breach at Oregon health care facility**



More Headlines

- **Lawmakers offer up several IT-security bills**
- **Every 79 seconds a thief steals someone's identity and goes shopping!**
- **HACKERS POST 30-40 NEW TOOLS TO THE INTERNET EVERY MONTH**
- **Aetna says computer with member information stolen**



Compliance strategies

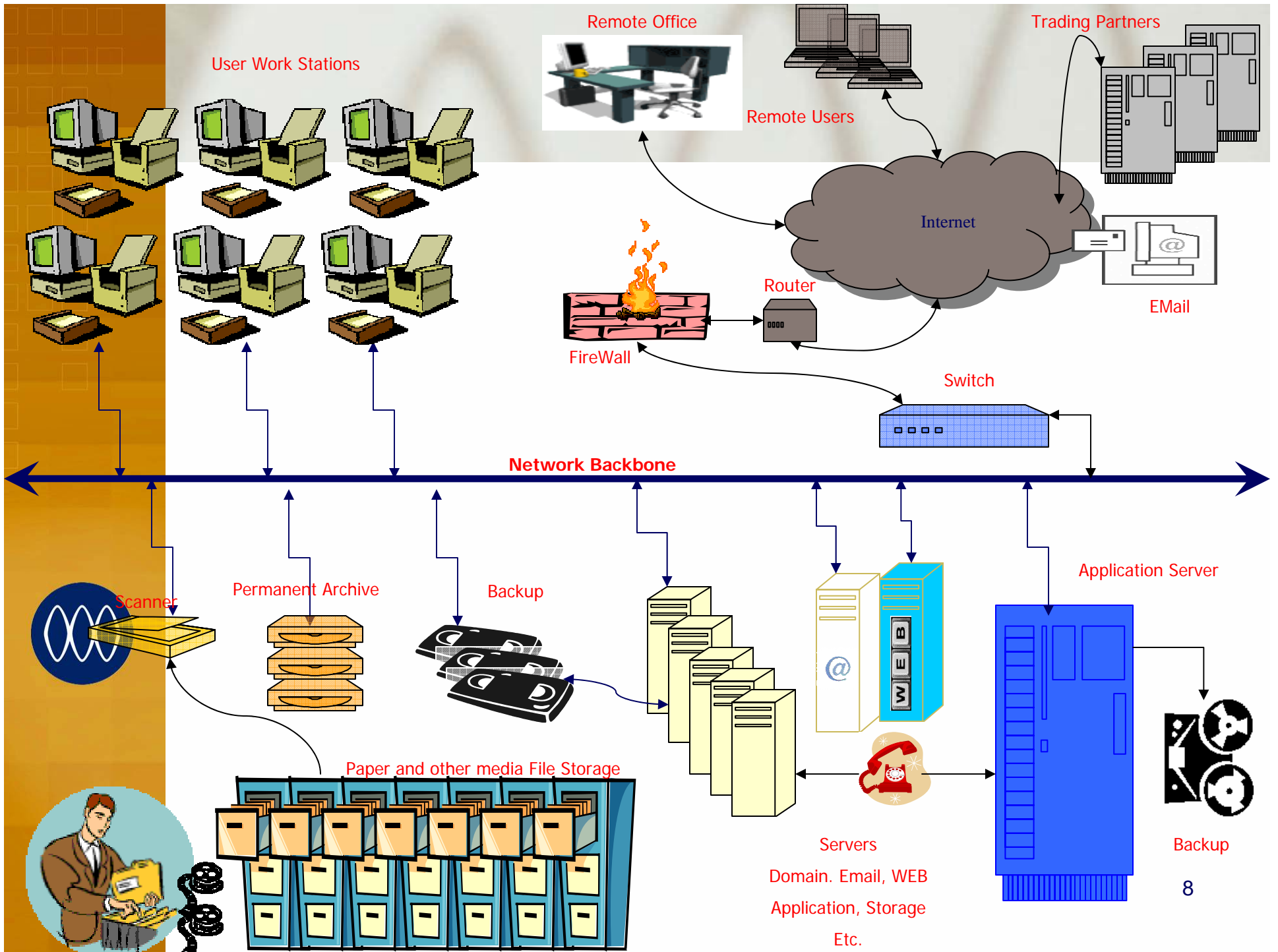
- Risk assessment to beat deadline
- Ad hoc crisis management
- Cool technical tools that help
- \$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$
- Delegate, delegate, delegate
- Just say YES



The Problem

- \$\$\$\$\$\$\$\$\$\$\$\$\$
- HIPAA §164.308 Administrative safeguards
 - Periodic evaluation
 - Security administration
- Organizational issues
 - Limited security expertise/interest of domain experts
 - Treatment as an IT problem not a management problem
- Too many moving parts (see next slide)
- How to decide when you are compliant





Lengthy Technical Security To Do list

1. Firewall and System Probing
2. Network File Systems (NFS) Application Attacks
3. Electronic Mail Attacks
4. Vendor Default Password Attacks
5. Spoofing, Sniffing, Fragmentation and Splicing Attacks
6. Social Engineering Attacks
7. Easy-To-Guess Password Compromise
8. Destructive Computer Viruses
9. Prefix Scanning
10. Trojan Horses
11. Malicious modification of hardware
12. Denial of Service (DoS)
13. Back-ups



AHIMA 2006 Survey

What was Upgraded?	Percent
Firewall	40.4%
VPNs	25.9%
SSL technology	12.8%
Anti-virus/spyware/spam	38.2%
Remote access: restricted access	25.3%
Remote access: caller ID	14.4%
Remote access: callback	13.7%
Remote ID and authentication	19.9%
Data back-up technologies	30.2%
RAID technology	13.3%
Cryptographic technologies	13.3%
Single sign-on	15.0%
Biometric technology	6.6%
Access control technology	14.1%
Intrusion detection monitor/response	10.6%



Hard to Control Stuff

- Administrative security
 - Governance
 - Policy and procedure implementation
 - Human resource practices
 - Reporting of suspicious activities
- Secure culture
- Physical security
- Ennui
 - Adequate disaster recovery planning
 - Periodic risk assessments



What administrative tools need to do

- Support bottom up security responsibilities
- Track compliance from the top down
- Provide lots of documentation
 - Audits
 - Risk Assessment results
 - Management reports
- Lower costs
- Assure state-of-the-art program
- Minimize disruption
- Manage process consistency



Other, different security tools

- Technical solutions
- Technical policy management tools
- Framework without any guts



What an Administrative System Is:


- Supports and maps controls to industry standards:
HIPAA • NIST • ISO • COBIT • ISSA
- Builds program base with detailed *Risk Assessment*
- Has a control library and built-in intelligence
- Permits customization
- Maintains documentation
- Manages diverse locations and IT platforms
- Identifies and controls remediation

Think: TurboTax




System Snapshot

https://ms2.milliman.com - The Security Management System - Microsoft Internet Explorer



Milliman



The Security Management System Welcome John !

Getting Started	Control Surveys	Compliance Assessment	Control Validation	Reporting Section
Resource Center	Administration	Information/FAQ	Logoff	

Task

- **Getting Started Instructions**
- Organizational Information
- Business Units Information
- Manage Organization Structure & Business Attributes
- Update Your Profile Information

Getting Started Instruction

WELCOME:

Thank you for using Milliman Security Management System (MS2).

Overview

It is easy to get your compliance assessment or program started.

Step 1
Before you define business units, Click on Organizational Information. Enter demographic information about your organization. (Note: This step is only done once when you initialize or when updates are needed.)

Step 2
Click on Business Units Information to add any subsidiary, business unit, department, or logical business process you wish to survey controls and risk assess for IT security compliance.

Note: You can add a Business Unit at anytime.


Step 3
Click on Update Your Profile Information to add your email address or make changes to your profile.

Step 4
Proceed to the Control Surveys Section or click on Control Surveys Tab at the top of the page. In that section you will select and assign control surveys for the organization and for each business unit that you define.




System Snapshot

https://ms2.milliman.com - The Security Management System - Microsoft Internet Explorer



Milliman



The Security Management System Welcome John !

Getting Started	Control Surveys	Compliance Assessment	Control Validation	Reporting Section
Resource Center	Administration	Information/FAQ	Logoff	

Task

- **Completing Survey(s) Instructions**
- Go To Organization Survey(s)
- Go To Business Unit Survey(s)
- Assign Survey(s)
- Show Status of Surveys
- Fast Track Control Survey Utility
- Advanced Custom Control Survey Features

Complete Survey(s) Instructions

Welcome:

Control Surveys Section

Introduction:

The Control Surveys section of the Security Management System is designed in an easy to use question and answer format structure. All questions either:

- Request simple yes or no answers, or
- Request you to add specific demographic info about your locations, vendors, business associates, and business application set, or
- Allow you to add any elaboration about your control in the remark field for all questions you answer YES to. This is optional but it is recommended that you use it when you want to clarify a control, for example, elaborate upon the implementation of a specific control.


For the organization and each business unit, you can select, delegate, and complete all the surveys that are relevant to your business circumstance.

Each questionnaire is intended to be short and should take from about 15 minutes to a maximum of 60 minutes to complete.

At the start of each control survey, we will summarize the information that you should be familiar with to successfully complete the survey. We will also estimate length of time it should take to complete.

Some conventions that you should know about:

- All questions need to be answered before a survey is completed; otherwise it will be labeled "in progress" as a status.
- System will automatically save all the information entered or questions answered.
- Navigation buttons are intuitive so you should have no problems navigating within the system.



Internet

System Snapshot

The screenshot displays a web browser window with two tabs. The background tab is titled "https://ms2.milliman.com - The Security Management System - Microsoft Internet Explorer". The foreground tab is titled "https://ms2.milliman.com - Questions - Microsoft Internet Explorer".

Task List (Left Panel):

- Completing Survey(s) Instructions
- Go To Organization Survey(s)
- Go To Business Unit Survey(s)
- Assign Survey(s)
- Show Status of Survey(s)
- Fast Track Control Survey Utility
- Advanced Custom Control Survey Features

Question # 1: Are the laptops used in this organization configured to require an ID and a password to logon to the device?

Back to: Question #1

Answer Options: Yes No

Remark: Most desktop operating systems such as NT, Windows 2000, and XP are or can be configured to require an ID and password to logon to the device.

Attach File: [Empty field]

Answering Question Guidance: Please answer YES, if you are at desired level. Answer NO, if either you are not at desired level or if this item is not applicable to your business circumstance. During Compliance Assessment, you will be able to address the NO items as appropriate.

Navigation: Exit, Previous, Next

System Footer: 2006 Milliman, Inc. All rights reserved. Various trademarks held by their respective owners. Milliman v.1.1.1.4

Browser Status Bar: Done, Internet



System Snapshot

https://ms2.milliman.com - The Security Management System - Microsoft Internet Explorer



Milliman



The Security Management System

Welcome John !

Getting Started	Control Surveys	Compliance Assessment	Control Validation	Reporting Section
Resource Center	Administration	Information/FAQ	Logoff	

Task

➤ **Compliance Assessment Instructions**

➤ **Go to Organizational Compliance Assessment**

➤ **Go to Business Unit Compliance Assessment**

➤ **Go to Organizational Compliance Tracking**

➤ **Go to Business Unit Compliance Tracking**

Compliance Assessment Instructions

Compliance Assessment Section

The Compliance Assessment section is also intended to be intuitive and the instructions to complete the Assessment are documented in the Security Management System software when you start the Compliance Assessment.

(Note: Compliance Assessment can ONLY be started after you have completed at least one control survey. We recommend that you complete all the control surveys for the organization or for a business unit before you start your compliance assessment, that way you will see all the alerts in context with the organizational entity, but compliance assessment can be completed as each survey is completed.)

The Compliance Assessment section is divided into three sub-sections:

• RED Alerts ▲

Red alerts are security gaps the system has categorized as potentially **"high risk"** that either should be corrected or document your rationale if this potentially high risk gap does not need to be addressed. (Note: You should document any mitigating factors or compensating controls.)

• Yellow Alerts ▲

Yellow alerts are security gaps the system has categorized as potentially **'medium risk'**. You will be prompted to either implement a security safeguard or document your rationale for not implementing. (Note: You should document any mitigating factors or compensating controls.)

• Blue Alerts or Other Opportunities ▲

Blue Alerts are security gaps that have been categorized as **lower** security gaps. You should review and address as appropriate.

To complete the Security Assessment section you must, at a minimum, address the Red and Yellow Alert items. We also strongly recommend that you also complete the Blue Alerts - Other Opportunities items. Addressing the items in this section is optional if



Internet

System Snapshot

Task

- Compliance Instructions
- Go to Organ Compliance A
- Go to Busine Compliance A
- Go to Organ Compliance T
- Go to Busine Compliance T

https://ms2.milliman.com - Compliance Item - Microsoft Internet Explorer

Gap Description :

At Business Unit (Business Process A)

A system ID and password is not required by remote workers to logon to their workstation. [Print](#) [View Answer to Question](#)

Recommendation Vendor

Description

Require remote workers to use a system ID and password to logon to their workstation.

Comment

Currently, operating systems such as NT, Windows 2000 & XP support user logon ID's and passwords. Enable this function. It establishes accountability for individuals using a workstation, protects against unauthorized use of the workstation and unauthorized access to data.

Yes, Add Recommendation to Action Plan

No, we do not plan to implement recommendation because of the following reasons:

Below are some suggestions that may apply to your business circumstance, please select all that apply and add any additional comments, if needed.)

Rationale List	Delete
<input type="checkbox"/> The size, complexity, and capabilities of this organization do not warrant implementing the security measures to address this specification.	
<input type="checkbox"/> The cost of the security measures required to address this control objective cannot be justified.	
<input type="checkbox"/> The risks at this organization are low that sensitive or confidential information will be breached because of the	

Done Internet

Remote workers are not required to have an 'uninterrupted power supply' (UPS) device to prevent loss of information from an electrical power disruption.

Remote workers are not instructed to secure associated documents that are maintained at their remote location for a business

Done Internet



System Snapshot

https://ms2.milliman.com - The Security Management System - Microsoft Internet Explorer



Milliman



The Security Management System

Welcome John !

Getting Started	Control Surveys	Compliance Assessment	Control Validation	Reporting Section
Resource Center	Administration	Information/FAQ	Logoff	

Task

Control Validation Section Instructions

Organizational Control Validation Section

Business Unit Control Validation Section

Control Validation Instructions

Control Validation Section

Please select the appropriate Organizational or Business Unit Control Validation button to proceed.

Otherwise, please read the Section Overview below to gain an understanding of this section.

Section Overview

The purpose of validating controls is to ensure that the control procedures that are in place are being complied to. Periodically validating controls is a good security and management practice, it is also a common audit practice; and finally, it helps ensure regulatory compliance. For example, there is a Sarbanes-Oxley (SOX) requirement that management regularly validate controls that are in place.

One of the benefits of the Security Management System is that the controls were validated through inquiry when the control surveys were performed. ("Yes" response to the control survey questions)

This section recaps the results of the control surveys and it is intended to be used to document any other control validation you have performed or wish to perform. You can also choose to qualitative rate the maturity level of the controls in place. (See below.)

At a high level, there are three ways to validate that a control is in place and it is being adhered to. You can validate controls by:

Inquiry:

Control surveys are an "inquiry" form of validation testing. By default, all the controls listed in the control validation section have been validated through inquiry.

Observation:

Visual inspection is a form of validating controls by observation. For example, inspecting physical controls such as displaying access badges by employees in the work area is validating a control through observation.

Testing:

Controls can also be validated by formally testing them. Testing is usually accomplished by using judgmental, statistical, or



Done

Internet

System Snapshot

https://ms2.milliman.com - The Security Management System - Microsoft Internet Explorer



Milliman



The Security Management System

Welcome John !

Getting Started	Control Surveys	Compliance Assessment	Control Validation	Reporting Section
Resource Center	Administration	Information/FAQ	Logoff	

Task

- Reports Section Information
- Compliance Reports
- Operational Reports
- Standards Mapping Reports
- Fast Track Control Reports

Reporting Section Overview

Reporting Section

This section contains all the necessary reports you will need to document your IT Security compliance effort

The Reporting Section contains three main areas:

1. Compliance Reports
2. Operational Reports
3. Standards Mapping Reports

Warning When you select "all" and you have many business units, some of these reports can be quite large and may take a few minutes for the system to generate the content. Most of these reports can be filtered at the business unit level.

Note A "business unit" associate will only be allowed to view reports for their business unit(s) and if they have "view report" rights.

1. Compliance Reports:

- **Policies & Procedures:** Lists all security policies and procedures either in place based upon the responses from the control survey or planned based upon the items you have chosen to address in the Compliance Assessment Section. (i.e. action plan items)

You can use this report for documenting and sharing Security Policies & Procedures.

Note: The reason that "planned items are reported" is because by generally accepted security standards, planned policies and procedures count to calculate your "security risk profile".

- **Compliance Tracking Report:** Lists all the items, recommendations or gaps you have chosen to implement in the



Done

Internet

System Snapshot

https://ms2.milliman.com - The Security Management System - Microsoft Internet Explorer



Milliman



The Security Management System

Welcome John !

Getting Started	Control Surveys	Compliance Assessment	Control Validation	Reporting Section
Resource Center	Administration	Information/FAQ	Logoff	

Task

- Reports Section Information
- Compliance Reports**
- Operational Reports
- Standards Mapping Reports
- Fast Track Control Reports

Compliance Reports

Report Name	View	Print
Policies and Procedures Listing		
Compliance Tracking Report		
Risk Assessment Summary Profile By Business Unit		
Business Unit Risk Summary Profile By Area		
Composite Risk Assessment Summary Profile By Area		
Business Unit Risk Assessment Profile By Threat/Vulnerability		
Composite Risk Assessment Summary Profile By Threat/Vulnerability		
Detail Risk Results and Controls Report		
Detail Risk and Gap Analysis Report		
Threat and Vulnerability Description Report		
Control Validation Detail Report		



Done

Internet

Implementation process

- Specify control needs
- Identify domain experts
- Set up organizational structure and users
- Users log-on
 - Report on existing controls
 - Describe “rationales” when specified safeguards are inapplicable
 - Commit to timeframe on planned controls
- Security manager follows-up to validate controls and manage process



Why these things work

- Common analytical framework
- Algorithmic approach
- Long history—multiple standard setting bodies
- Regulators borrow from accepted standards
- MS SQL makes for easy database management



Administrative System Criteria

- Routine comprehensive assessments
- Due diligence documentation
- Management level reports
- Good library of controls
- Multipurpose applicability
- Easy to implement
- Multiple-sites/multiple users
- Support for domain expert contributors
- Simple risk assessment process



Examples

- Decentralized organization with multiple locations
 - Need for minimal intrusion on local operations
 - Limited field security expertise
 - Provision for consolidated, auditable results
- Business associate with IT but no security specialist
 - Tight margins
 - Responsibility to covered entity clients



Conclusion

- Administrative simplification requires automation of administration
- Granular security alone is not sufficient
- Administrative tools exist to provide a security program that is:
 - Comprehensive
 - State-of-the-art
 - Manageable
 - Affordable
 - Compliant



Automating Security Administration

Are We There Yet?



John L. Phelan, Ph.D.
Management and Technology Consultant
Telephone: 818/707-7818
E-mail: john.phelan@milliman.com

