Case Study: Information Security Awareness at LS&CO.

Paula Moore, CISSP
Levi Strauss & CO.

CSI-Asia Conference
October, 2004

Time for a Break….

- This is the last presentation of the day
- Are you?
  - A. Energized and excited about all the things you have learned today
  - B. Apprehensive and a bit overwhelmed about all the things that you will have to do as a result of the things you have learned today
  - C. Tired and needing a break
  - D. All of the above
- Here is a question that will let you have some fun before we discuss

"Security Awareness"

Top 10 reasons for security awareness

- **What are the Top 10 reasons for a security awareness program at your organization?**

Top 10 reasons for security awareness

- # 10 - Heard about “it” in Information Security magazines
- # 9 - Other companies are doing it so it must be “the right” thing to do
- # 8 - You have budget money left after all the important projects!
- # 7 - Awareness posters provide inexpensive “art” for office walls

Top 10 reasons for security awareness

- # 6 - CSI-Asia made me say it
- # 5 - Microsoft Trusted Computing
- # 4 - LOphtCrack
- # 3 - Internal Audit is watching
- # 2 - New product ready for market
- # 1 - BUT…….

Top 10 reasons for security awareness

- # 1

Your competition beat your new product to market by 2 weeks!!!

Which of these apply to you?

Presentation Goals

- Recognize challenges to information security programs and how to overcome them
- Define the building blocks of an information security awareness program
- Define specific deliverables for each building block
- Avoid mistakes in implementing a successful security awareness program
- Identify awareness tools, techniques, and messages that work well

Summary of Discussions Items

- LS&CO. Overview
  - LS&CO. IT and Security Organizations
  - Operational Security Model
  - Corporate Culture
  - Risk/Roadmap
- Challenges to Information Security Programs
- Building a Security Awareness Program
- Conclusion
- Questions

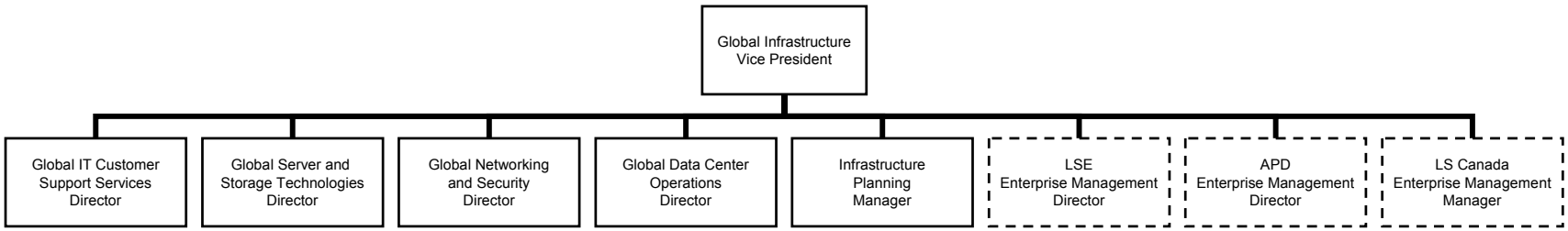
LS&CO. Overview

- Founded in 1853
- Sales in over 100 countries; organized into 3 geographic regions
  - America's (headquartered in San Francisco)
  - Europe (headquartered in Brussels)
  - Asia Pacific (headquartered in Singapore)
- 11,000 people worldwide (1,250 in San Francisco)
- 3 brands
  - Levi's®, Dockers® and Levi Strauss Signature™

Security Organization Reporting Structure

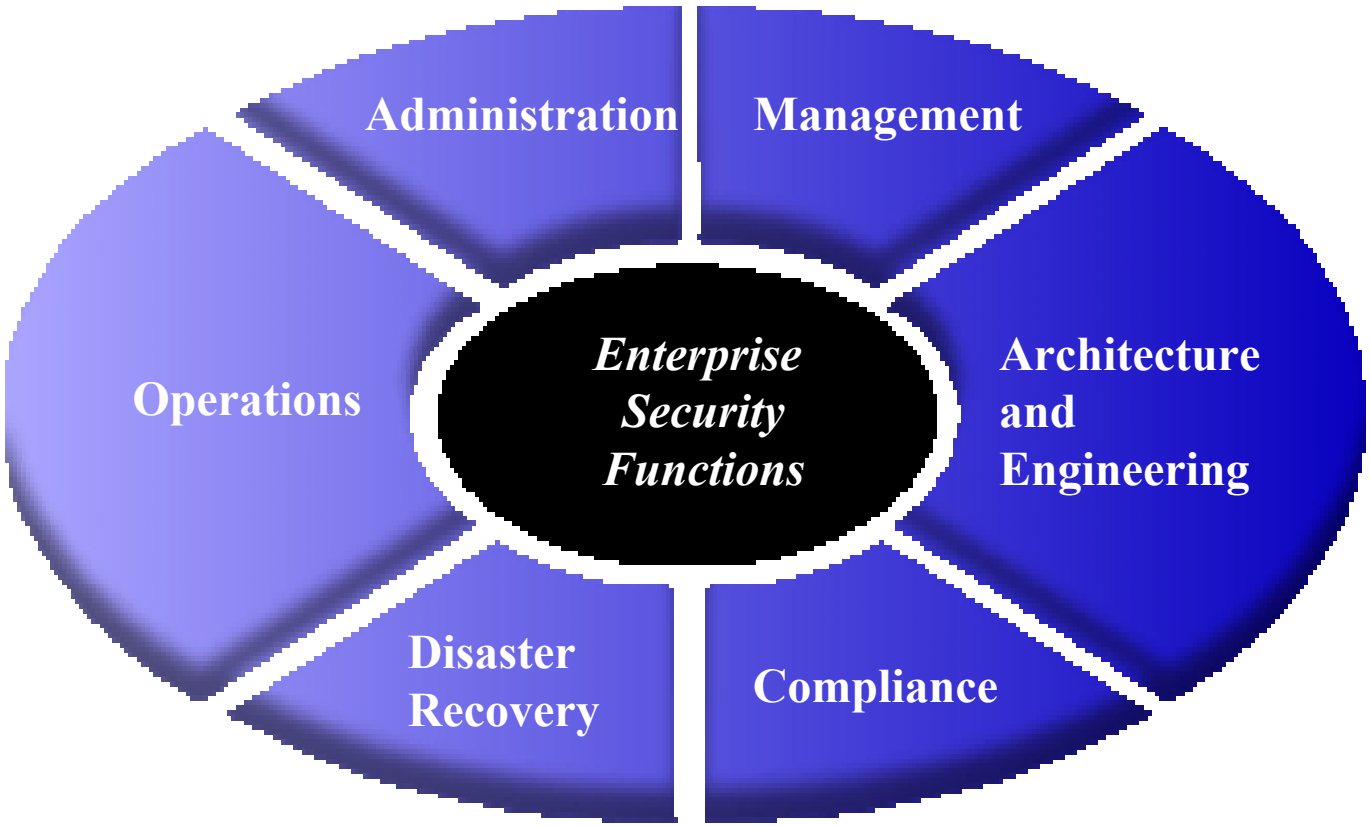
- Your organization's reporting structure is an important aspect to consider before you design your security awareness program
- Why?
  - Sponsorship
  - Funding
  - Approval
  - Compliance

LS&CO. Global Infrastructure Organization



- **Global IT Security functions and responsibilities**
  - Strategies, policies, standards and guidelines
  - Risk assessment and mitigation
  - Consulting
  - Architecture, engineering and operations
  - Information Security Response Program
  - Security administration
  - Security awareness

Enterprise Information Security Framework



** Based on Best Practices in Managing IT Security (GIGA Planning Assumptions -March 2002)*

Operational Security Model

- Business Focused
- Protect the confidentiality, integrity and availability of information
- Security is a functional silo but spans across other silos
- “Enable” not “disable” business

Operational Security Model

- End-to-end security
- Inform and educate – do not preach or instill fear (well maybe a little)
- Agility
- Risk Driven – identify and manage risk

Key Risk – Why Implement Awareness?

The Key Risk is…..

… information is not effectively protected, controlled and managed to ensure availability and accuracy for key decision making and financial and regulatory reporting.

LS&CO. Risk Mitigation Roadmap

LS&CO. focused on key initiatives to address risk:

- Security strategy and architecture
- Information Security policies and standards
- Risk analysis process
- Operational procedures to ensure production integrity
- Secure systems - prevention, detection, monitoring, logging
- Metrics

LS&CO. Risk Mitigation Roadmap

LS&CO. focused on key initiatives to address risk:

- Security checkpoints in SDLC (Systems Development Lifecycle)
- Identity and User Account Management
- Awareness Program …..

….. Security Awareness affects the bottom line!

Challenges for Information Security Programs

- **Security is seen as a hindrance to productivity**
- **No organizational champion; weak reporting structure**
  - Scope and authority will be challenged
- **Corporate culture – know yours!**
  - Open and collaborative may be more resistant
- **"We're not a bank" so we don't have anything of value/lack of awareness**
  - Famous last words….
- **Shrinking budget**

Building a Security Awareness Program

- **Assess Corporate culture affect on awareness goals**
- **Research successful security awareness programs**
- **Sponsorship – find a champion for your cause**
- **Set clear and realistic goals for the program**
- **Create a program map – project management is a necessity**
  - Security Awareness Program plan
  - Content and delivery process
  - Rollout

Building a Security Awareness Program

- Communications
- Implement / Review / Renew

Corporate Culture Affect on Awareness

- **LS&CO.'s work environment**
  - Market driven – business re-engineering
  - Resource "light" and "young"
  - Fast-paced
  - Strong corporate values
    - Empathy – walk in another's shoes (consumer's too)
    - Originality – be authentic and innovative (create trends)
    - Integrity – doing the right thing (responsible commercial success)
    - Courage – standing up for beliefs (challenge convention)
- **Why is it important to know yours?**
  - Security awareness isn't an end in itself – how you get there depends on the organizations **values** and **ways of working**
  - Know your constituents and their communication style
  - Determine the organization's attention span – how soon do things become "old news"

Corporate Culture Affect on Awareness

- **LS&CO.'s Key Learning's**
  - Awareness messages could not be "IT-like"
  - Awareness delivery had to be "woven" into existing work, projects, and processes because everyone was too busy to pay attention to one more thing (especially from IT!)
  - Awareness messages had to be targeted to real-life experiences
  - The delivery method that worked best was the one that people paid attention to the most – the web!
  - Quote Policies and Standards sparingly
  - To reach a common understanding, messages needed to be simple, relevant, clear and concise

Research

- **Research the obvious and not so obvious places**
  - CSI, Gartner, META (or your favorite flavor consultant)
  - Network and consult with peer companies
  - Identify other “awareness” efforts in place at your company and how they work
    - How is the weekly menu for your company cafeteria communicated?
- **LS&CO.’s Key Learning's**
  - An attention-getter was needed to draw initial interest
  - Searching out the not so obvious “awareness” efforts kept the overall vision in balance
  - Keep exploring resources to re-validate and learn

Sponsorship

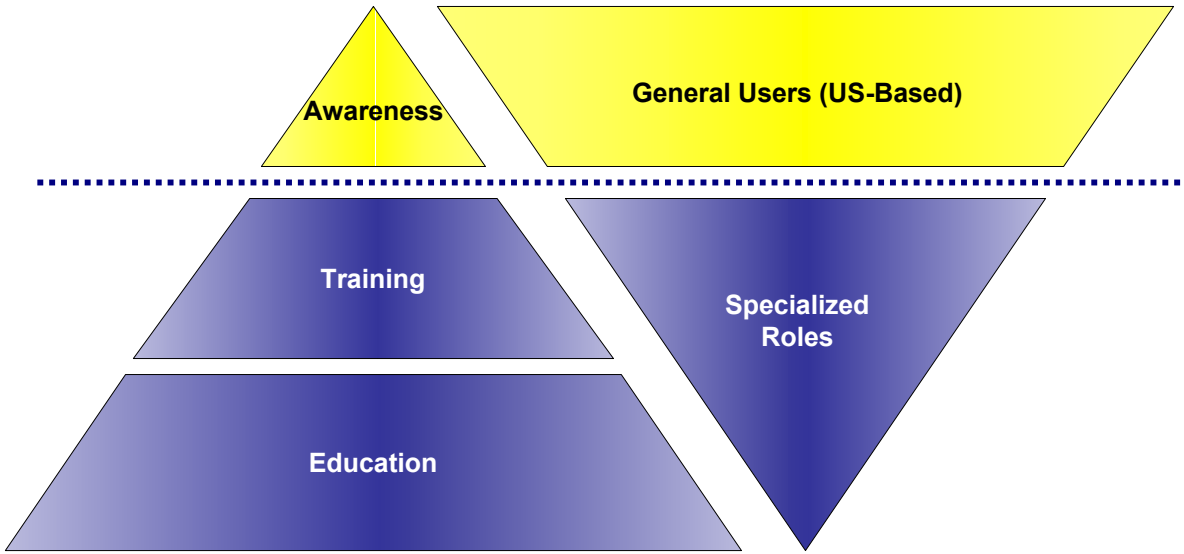
- **Sponsorship-isms**
  - A Corporate-wide and Global awareness program needs a sponsor with influence
  - Deploying in a phased approach requires sponsorship re-introduction and the inclusion of local or regional sponsors
  - Keep your sponsors well informed of progress/success and identify barriers that need the sponsor's help – tell the "story"
- **LS&CO.'s Key Learning's**
  - IT sponsored but the business was the "champion" or true sponsor
  - The "story" needs a central theme or "icon" to keep it familiar

Define Program Goals

- **Set clear and realistic goals for the program**
  - Define “awareness”
  - Involve your stakeholders up-front in planning and verifying scope
  - Visualize your “peak” and the map the critical points your need to reach to get there
  - Start small and build
  - Awareness is a process – not an end-state
- **LS&CO. Key Learning’s**
  - Validating the scope early and more clearly could have prevented confusion among stakeholders, which sidetracked our goals and delayed some initial work

Security Awareness Objective

"Keep employees mindful of their responsibility to protect company assets from harm or loss"



- **Awareness Objective:** Focus attention on security

  Communication of information security topics to current employees and new employees

- **Training Objective:** Produce needed security skills

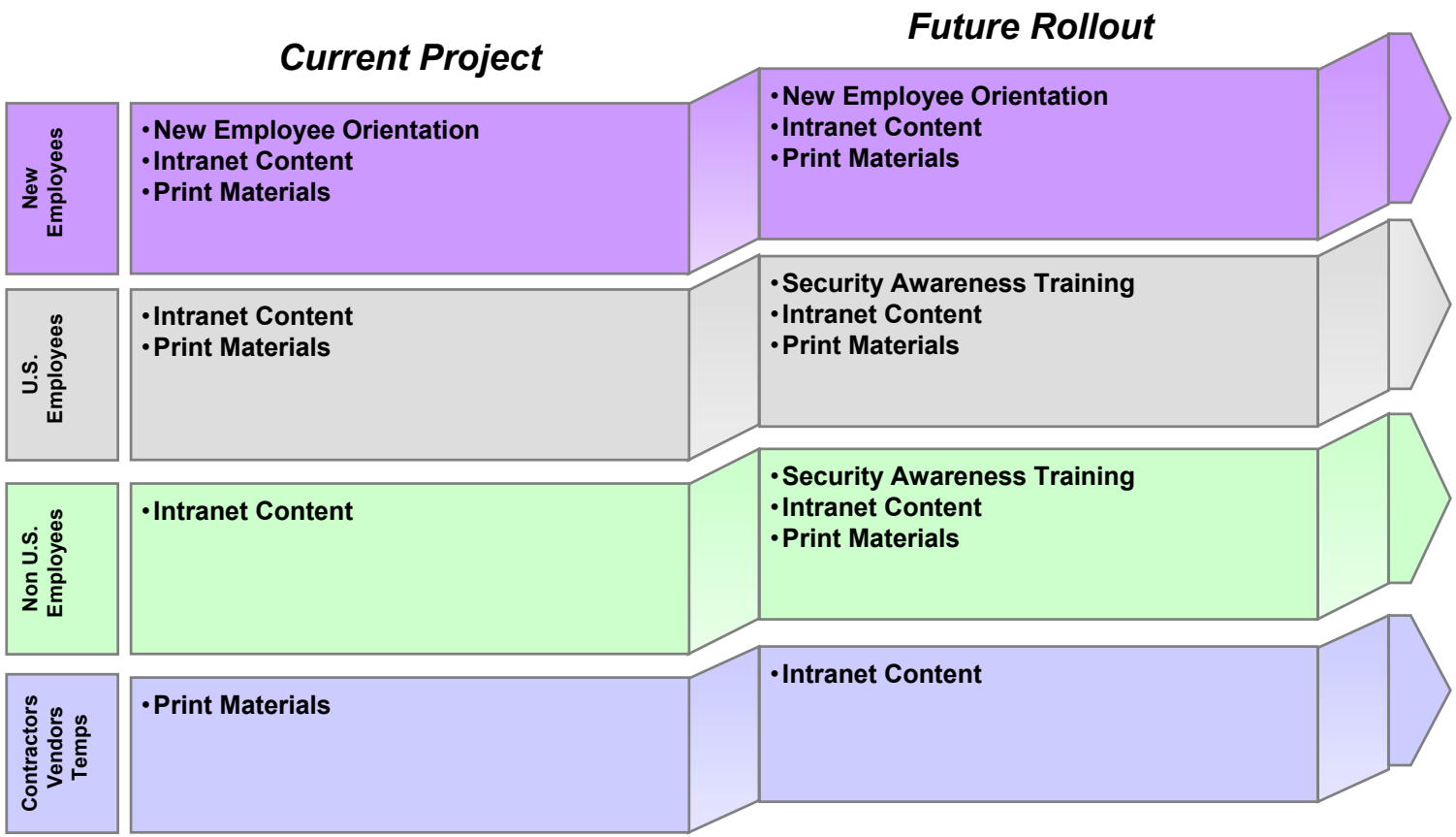
  In-depth training delivered to specific roles including Network and UNIX Administrators

- **Education Objective:** Produce IT security specialists

  Comprehensive and integrated security education delivered through Certification and University programs

Project Scope

The implementation of the Security Awareness Program across the organization took a phased approach.



Project Overview

	Phase 1	Phase 2	Phase 3
	Security Awareness Program Development	**Security Awareness Program Implementation**	**Security Awareness Program Rollout**
Program	*Security Awareness Program Plan*		*Revised Security Awareness Program Plan*
Process	*Security Topic Selection/Validation*; *Awareness Delivery Selection/Validation*	*Security Content Development and Refinement*	*Awareness Content Publishing*; *Awareness Delivery*; *Awareness Tracking*
Planning and Communication	*Revised Project Schedule*; *Communications Plan*	*Security Awareness Program Implementation Plan*	

Key Project Activities and Deliverables

Phase	Awareness Program Development	Awareness Program Implementation	Awareness Program Rollout
Activities	• Update project schedule (Workplan) • Identify project dependencies • Identify user groups and needs • Develop communication plan • Identify roles and responsibilities • Identify methods for delivering awareness materials • Identify and validate security awareness topics • Identify Intranet content requirements • Document Security Awareness Program Plan • Obtain manager review of Awareness Plan • Update and finalize Security Awareness Program Plan	• Develop Security Awareness Program Implementation Plan • Support the development of initial security awareness materials • Obtain manager review of Security Awareness Program Implementation Plan • Update and finalize Security Awareness Program Implementation Plan	• Publish security awareness materials on the Intranet • Deliver security awareness messages to delivery method owners
Deliverables	• Revised Project Schedule (MS Workplan) • Communications Plan • Security Awareness Program Plan	• Security Awareness Program Implementation Plan • Recommended Security Awareness Materials	• Revised Security Awareness Program Plan

Communications

- **Is it too obvious to say that awareness communications requires a communications plan?**
  - Work out the plan together with your Corporate Communications department – use their expertise to tell your “story”
  - Define your communications channels to deliver awareness content
  - Match the delivery channel to the constituency; map to their communication style
- **LS&CO. Key Learning’s**
  - Using existing communications channels saved time and work and eliminated complexity
  - Using business resources to deliver awareness messages where needed insured a match to communication styles

Implement/Review/Renew

- **Follow the program implementation plan**
  - Keep the communications and implementation plans in synch
  - Document what works and what doesn't - pay attention to pain points, too
  - Learn and re-work the plan, process, delivery, communications, etc.
- **LS&CO. Key Learning's**
  - The implementation would not have been successful without flexibility and commitment to adjust the plan even though we thought we had the best one
  - The process will evolve with changes in the organization, security and technology
  - The sponsor wanted a "security trinket" as part of the plan; don't forget to budget for it!

Implement/Review/Renew

- **LS&CO. Key Learning's**
  - Awareness would have to build slowly and start with a change in perception; less rigorous than originally planned
  - Other company initiatives were infused with awareness messages; more subtle than originally planned
  - We did not anticipate the impact of a downsized organization on program operation

Key Wins

- **Implemented security awareness messages**
  - Confidentiality Website
  - COE 4.0 XP Reference Manual

- **Developed key relationships with and received support from business units for future collaboration efforts Worldwide and U.S. Communications, Worldwide HR, Worldwide Security**

- **Addressed Internal Audit's requirement for communicating security awareness to LS&CO.**

- **Our definition of "awareness" was correct**

- **Management has stayed interested**

Update – Year One and Counting

- **LS&CO. Key Learning's**
  - Awareness program plan template was tailored for use in our global locations; some processes were used consistently and some were not
  - An awareness program is important to maintain during organizational change and business change, so look for ways to optimize
  - Create mechanisms to measure success and failures
    - "Awareness" is difficult to quantify so look for other measurements that will provide information and clues as to where the organization needs targeted awareness messages

Global Information Security Metrics

	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov
Security Notifications - GIS												
Number of Notifications	0	0	0	0	14	0	2	20	46			
Average Time to Apply Critical Patches (in Days) - Target is 14 Days												
MS04-022/23												
US Desktop									7			
US Server									14			
LSE Desktop									14			
LSE Server									14			
APD Desktop									**55**			
APD Server									**55**			
Sygate Firewall - Blocked Intrusions (Deployed in US and APD)												
High Risk Events (i.e. MS Blaster Worm)									1194			
Medium Risk Events (i.e. Sasser Worm)									3517			
Unauthorized access attempts (i.e. probes or hacks)									7415			
E-Mail Files Quarantined and Cleaned												
Internal Exchange Servers									57			
In-bound at Internet Mail Gateway									22719			
Spam Blocked (Number of Messages)												
88% of in-bound Internet Mail									3.52M			
Spyware Incidents (Number of Help Desk Support Calls)												
US									102			
APD - begin report 10/04												
LSE - begin report 10/04												
WebSense (number of blocked Internet sites due to policy) * Graph on next page												
Hits (page request) blocked by policy									62K			

Conclusion

- Define what “awareness” means for your organization
- Know your Corporate culture
- Keep awareness messages simple, clear and relevant
- Define your scope, sponsor and plan and be flexible to change
- Use key relationships to keep the program fresh and in-synch with the organization
- Create a program template; tailor for deployment in other regions
- Start small and build; implement locally and then globally
- Create mechanisms to measure success and failure and keep updating your plan

Questions

?????

Paula Moore

Pmoore2@levi.com

415-501-7570