Building and implementing an effective Information Security and Privacy Awareness and Training Programme

JUCC

Dickson Wong, Hospital Authority

19-20 May 2011

Common Misconceptions on Training Programme

1. Training separated for Information Security, Privacy, or Records Management etc
   - From CSO, CPO etc
   - Thus inconsistent and confused employees
2. Treating campaign as the programme
   - Campaign is one-off
   - Programme shall be refreshed

From Jay Cline, Computerworld 2010

Common Misconceptions on Training Programme

3. Equating awareness to Training
   - Email sent to all, a powerpoint on Intranet, a
   - Need customized role based training
4. One or two communication channels
   - We lived in multimedia world
   - Need to include richer content, e.g. Interactive training
5. No measurement
   - Need to evaluate effectiveness of training

From Jay Cline, Computerworld 2010

Background

- People are one of the weakest links when attempt to secure systems and networks.
- The “people factor” - not technology - is key to providing an adequate and appropriate level of security
- A robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

HA's Workforce

Category	#
Medical (Doctors)	5000
Nurses	20000
Allied Health	5000
Others (Supporting Staff)	25000
Total	>55000

Information Security & Privacy Risks

- Unauthorized disclosures, modification, destruction of information
- Inadvertent modification / destruction
- Denial or degradation of service
- Violation of the Personal Data (Privacy) Ordinance

Information Security & Privacy Risks

- Through :
  - People
  - Applications, software & operating system
  - Communications & Network
  - Facilities & Equipment

Individual Responsibility

1. People are poorly trained / poor security awareness
2. People know the security requirements but are not motivated to perform
3. People are aware of security problem but as managers / employees making poor decisions
4. People can also malicious and do harm to organization

From SANS Institute

Classic Example - ATM

Spot the difference…Can you tell now?

- **Top photo shows an unadulterated ATM fascia. The flashing lead through entry indicator is easily observed.**

  Note: Most skim devices when fitted will obscure the flashing entry indicator this should be a vital clue as to any suspect tampering.

Spot the difference in the next photo.

- **A skim device has been placed in or near the card reader slot. Although the device has been given the appearance of being a standard part of the terminal it is in fact and additional fitted piece & clearly is different from the above photo.**

  Note: No flashing lead through light can be seen.

  The shape of the bezel is clearly different.

ATM Fraud – User Training

Here we have another example of the skimming device being piggy-backed onto the card reader

Policy

- *"Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall ensure that employees are versed in the rules of the system . . . and apprise them about available technical assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system."*

From NIST SP 800-50

Federal Information Security Management Act (FISMA) of 2002

- FISMA also states that the required "*agency wide information security program*" shall include "*security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of:*

- *(i) information security risks associated with their activities; and*

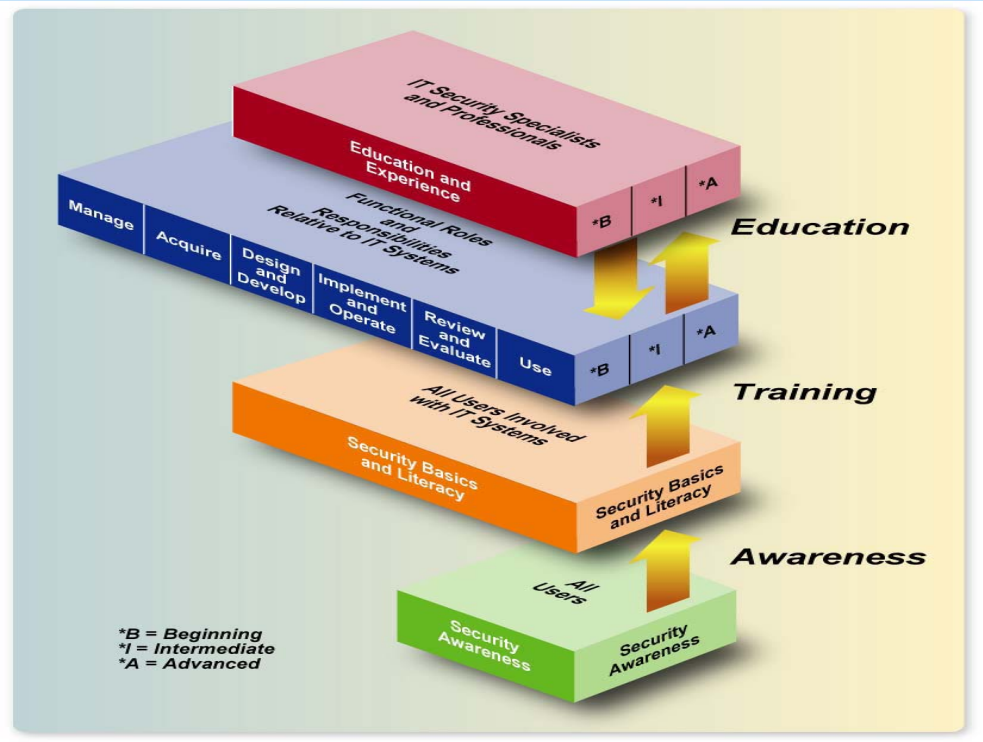
- *(ii) their responsibilities in complying with agency policies and procedures designed to reduce these risks"*

Security & Privacy Programme

Awareness and training program

1. roles and responsibilities,
2. development of program strategy,
3. development of a program plan,
4. implementation of the program plan,
5. review of the awareness and training program.

The IT Security Learning Continuum(1)



Learning is a continuum; it starts with awareness, builds to training, and evolves into education.

From NIST SP800-50

The IT Security Learning Continuum (2)

Awareness

- Security awareness efforts are designed to change behavior or reinforce good security and privacy practices, to focus attention on security, recognize IT security concerns and respond accordingly.

Training

- Training strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security

The IT Security Learning Continuum (3)

Education

- Education integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge . . . and strives to produce IT security specialists and professionals capable of vision and pro-active response.

Professional development

- Professional development is intended to ensure that users, from beginner to the career security professional, possess a required level of knowledge and competence necessary for their roles.

Development of an IT security awareness and training program

3 major steps:

- designing the program (including the development of the IT security awareness and training program plan),
- developing the awareness and training material, and
- implementing the program.

Structuring an Awareness and Training Program

- An awareness and training program may be designed, developed, and implemented in many different ways. Three common approaches or models are described below:
  - Model 1: Centralized policy, strategy, and implementation;
  - Model 2: Centralized policy and strategy, distributed implementation; and
  - Model 3: Centralized policy, distributed strategy and implementation.

Model 1 – Centralized Program Management

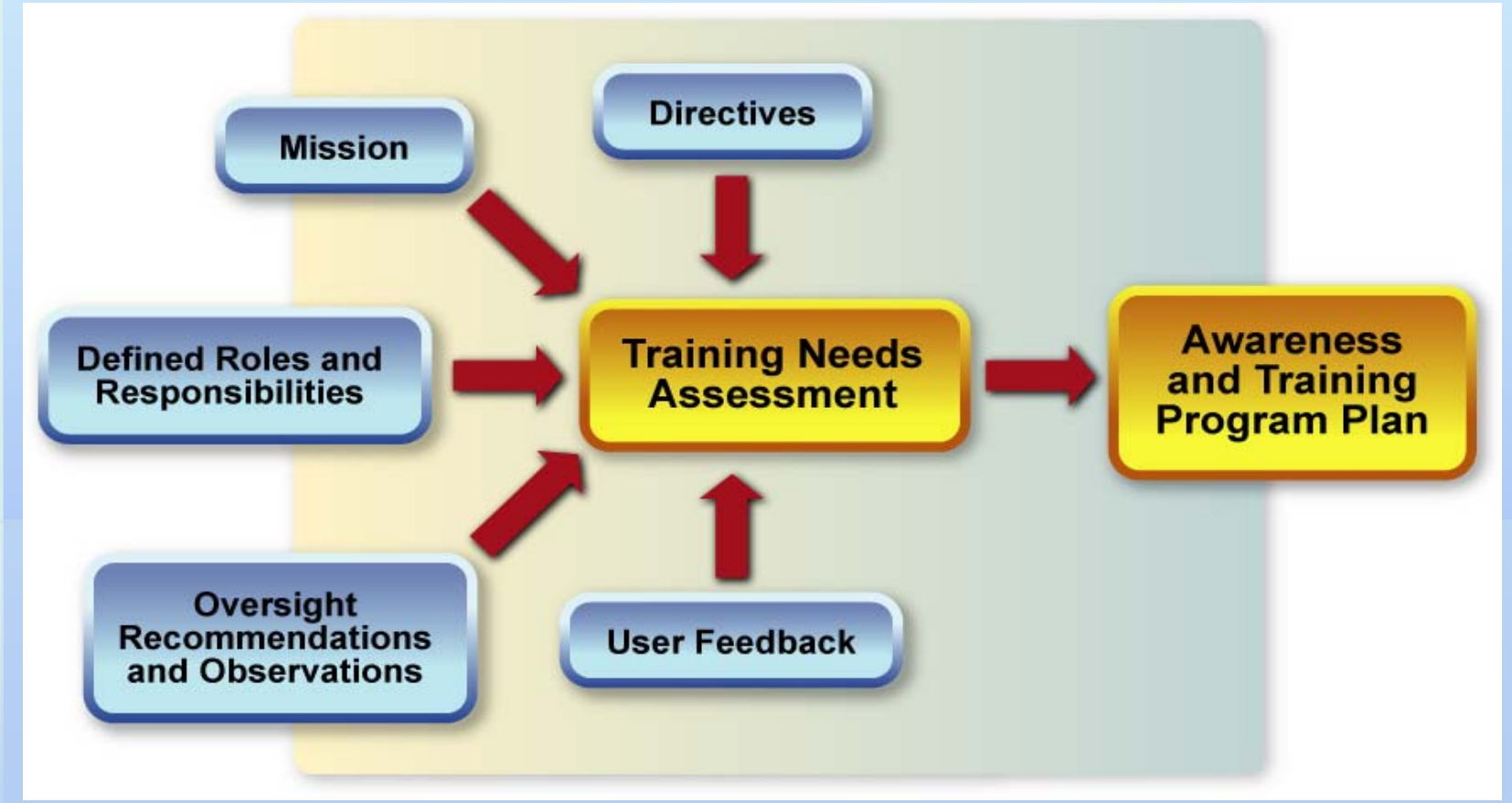
Model 2 - Partially Decentralized Program Management

Model 3- Fully Decentralized Program Management

HA's Experience

- Centralized - A uniform security and privacy training implementation
  - Standardized expectation on how employee should follow the policy and procedures
  - Common emphasis on risk areas
  - Monitoring compliance – no argument
- Basis of development of compliance framework

Conducting a Needs Assessment



Awareness and Training Strategy and Plan (1)

- Executive Summary
- Background
- IT Security Policy
  - Goals
  - Objectives
  - Roles/Responsibilities
- Awareness
  - Audience (management and all employees)
  - Activities and target dates
  - Schedule
  - Review and updating of materials and methods

Awareness and Training Strategy and Plan (2)

- Training/Education

Role 1: Executive and Managers
Role 2: IT Security staff
Role 3: System/Network Administrators & remaining roles w/ significant IT Security responsibilities

- Learning Objectives
- Focus Areas
- Methods/Activities
- Schedule
- Evaluation Criteria

- Professional Certification

Role 1: IT Security staff
Role 2 : System/Network Administrators & remaining roles w/ significant IT Security responsibilities

- Learning Objectives
- Focus Areas
- Methods/Activities
- Schedule
- Evaluation Criteria

Awareness and Training Strategy and Plan (3)

Resource Requirements	Cost
↳Staffing	$ xxx
↳Contracting Support	$ xxx
↳Facilities (e.g. training rooms, teleconferencing facility)	$ xxx
↳Media (e.g. server(s) for web- and computer-based material)	$xxx

Strategy of Delivery

- Outsource / in-house
  - Training material development
  - Training delivery
- Maximizing Partnerships
  - With external prominent parties e.g. PCPD
- Web-based training platform
  - Interactive, Clear, Consistent and Effective
- Separate content for different employee groups

Strategy of Delivery

- Training aims:
  - Policy Objectives
  - Organizational commitment
  - Expectation on employees, including discipline
- Produce security and privacy skills and competencies

Existing Awareness programs

1. Essential elements on protecting patient data privacy and security (both English & Chinese)	
Audience	**all HA Staff** (both clinical & non-clinical)
Activities	e-Learning on HA intranet http://elc.home/
Target dates	year end
Schedule	every 18 months, for serving staff and mandatory into the pre-internship learning package
Review & updating of materials & methods	Attendance summary report for review. Material update every 18 months or when there are new ordinances and business requirements

2. Privacy and Security Training Kit for General Staff VCD	
Audience	**General Staff**
Activities	VCD distributed to all Clusters
Target dates	year end
Schedule	every 18 months for serving staff
Review & updating of materials & methods	Attendance summary report for review. Material update every 18 months or when there are new ordinances and business requirements

Existing Awareness programs

3. Video - 保障病人私隱 醫護人人有份 **Protect yourself, Protect your patient - Data security is everyone's job**	
Audience	**all HA Staff**
Activities	Broadcasting in HA Channel wef 29 May 2008
Target dates	
Schedule	
Review & updating of materials & methods	

4. Briefing rounds on "good security practices and PDPO" to Clusters	
Audience	**All HA Staff**
Activities	Cluster rounds
Target dates	year end
Schedule	
Review & updating of materials & methods	Material update every 12 months or when there are new ordinances and business requirements

New Awareness program to be developed

Video on Information Security and Privacy of Patient Data in HA (8-12 minutes)	
↳Audience	**all HA Staff**
↳Activities	Video distributed to clusters
↳Target dates	
↳Schedule	
↳Review & updating of materials & methods	

↳Audience	
↳Activities	
↳Target dates	
↳Schedule	
↳Review & updating of materials & methods	

Review of Training Programme

- Monitor the Compliance and Effectiveness
  - Spot check for compliance (compliance checklist)
  - Security & Privacy Review
- Evaluation and Feedback
  - HA clinicians and staff are busy professionals
  - Focus Groups to collect evaluation & feedbacks

Way Forward

- Training is an ongoing task to change security and privacy culture (raising the standard)
- Training content to tailor for classes of employees
- Monitoring of Compliance