terranova
SECURITY AWARENESS

Lise Lapointe
President
www.tnsecurityawareness.com

Agenda

1. Industry Facts
2. Planning for Success
3. The Project factor
4. Project Planning
5. Setting Goals
6. Gathering the team
7. Determining Content

terranova

Industry Facts

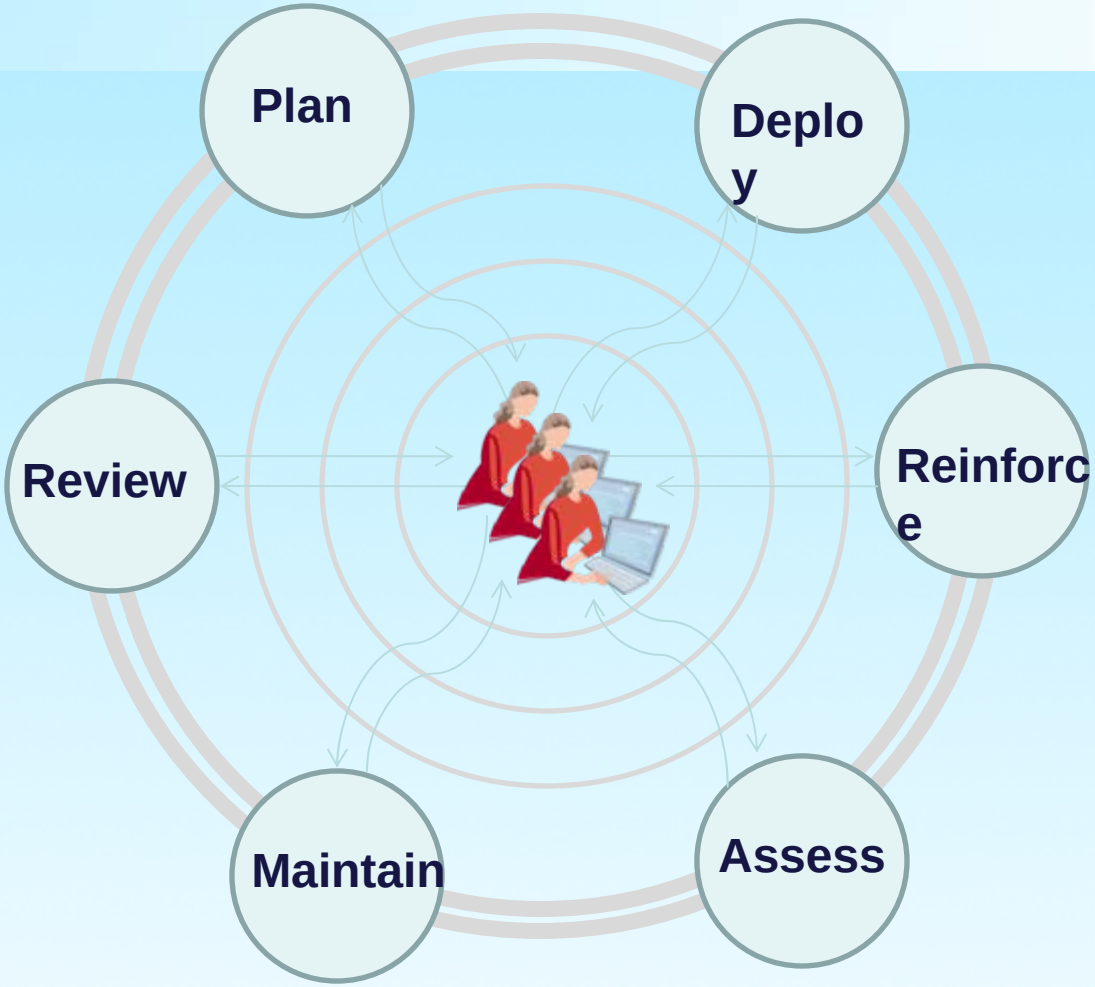
- Ernst & Young 2008 Security Survey -10 key findings - #6 People remain the weakest link for information security
- Deloitte's 6th annual Global Security Survey 2008 - people are the problem when it comes to keeping things secure.

terranova

Planning for Success

- Most organization's engage in ISATP because they need to meet certain guidelines or compliancy standards.
- What many fail to realize is that in order to change employee behaviour within an organization you need to be training continuously.

terranova



terranova

The Project Factor

- Treat ISATP like any other information technology project
  - Define the project scope
  - Assign a project manager
  - Recognize a project champion

terranova

Project Planning

- You need to create a project plan document that includes defining business objectives and scope
- Produce a clearly defined document and appoint those who will be held accountable.
- This document will become the guide for planning, implementation and ultimately measuring the effectiveness of the ISATP outcomes.

terranova

Setting Goals

To ensure you are working toward the right goals, you will want to ask the following:

1. What is the company's security strategy
2. What info needs to be protected and how sensitive is it?
3. What regulatory constraints apply (MITS, PCI, SOX?)
4. What are the company's security policies and how are they translated into daily activities?

terranova

Setting Goals

5. How does security affect employee's day to day activities.
6. How would a major security incident effect the organization?
7. What are the critical business processes in the company?

An internal message needs to be developed that is unique to the company culture, the industry and the regulatory climate. The message must then be communicated as part of the overall plan.

terranova

Gathering the team

- Project Manager - responsible for coordinating project activities.
- Project Champion - provides vision and management support for security awareness. This is typically the individual known to have ultimate authority and responsibility in regards to information security throughout the organization.
- The project team NEEDS to consist of all appropriate stakeholders within the organization or department.

terranova

Baseline and Content Considerations

- Use internal security policies and guidelines as well as best practice guidelines
- Establish a baseline of knowledge
- NIST provides some good guidelines (NIST SP 800-50) which include:
  - Recent incidents
  - Regulatory issues
  - Employee concerns
  - Management concerns
  - Customer concerns

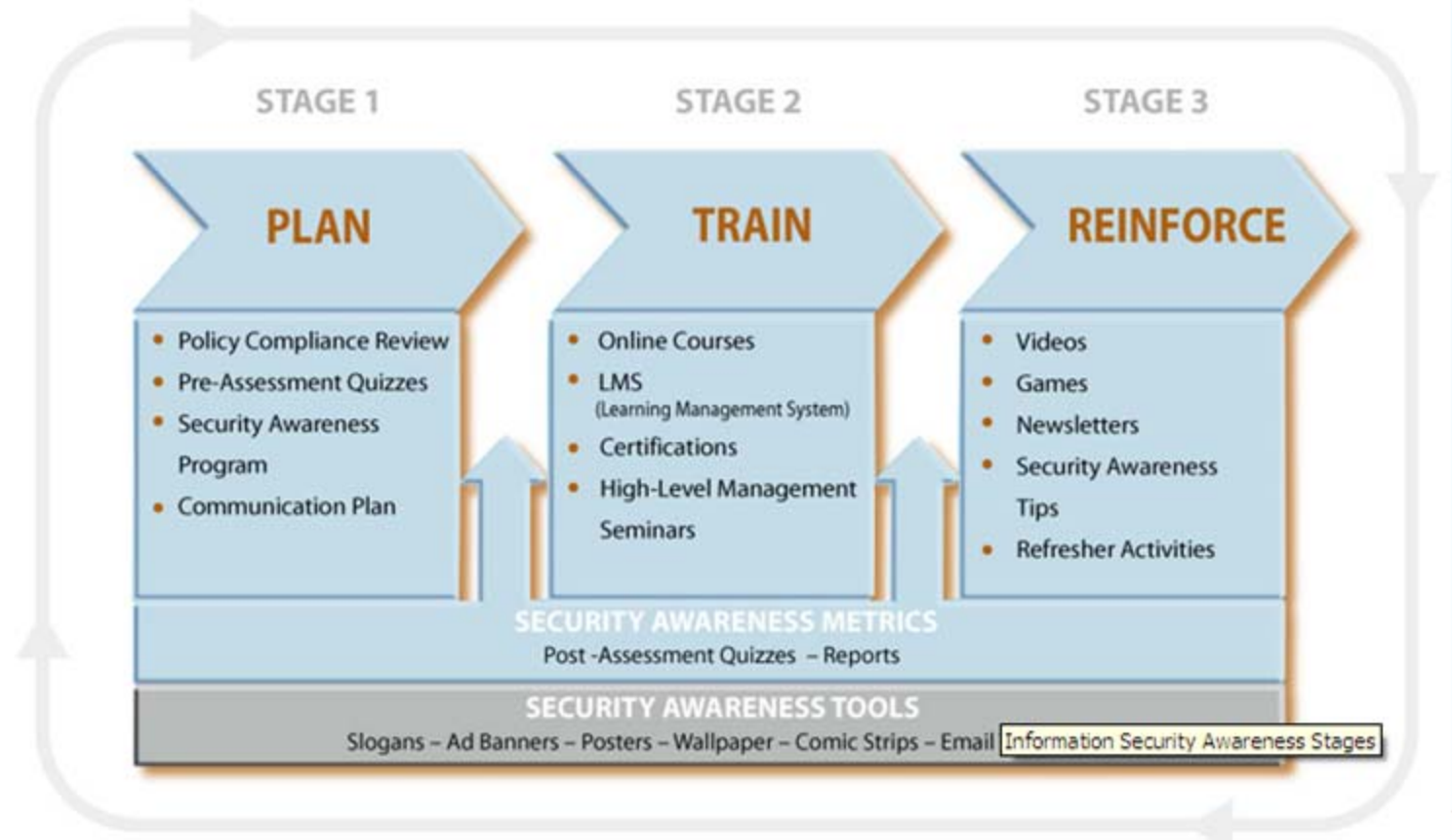
Determining Content

- Developing content internally can be both time challenging as well as expensive.
- A good off the shelf package can help you save time and money. It should provide best practice training for both end users, management and IT staff.
- The courseware should be delivered as-is, or customized to meet the needs of the organization's unique culture.

terranova

Our Approach

An awareness campaign is the foundation of an effective information security program.



terranova

ISATP Planning

- Security Awareness Assessment:
  - Quiz
- Design the training to meet the company's specific needs:
  - Type of clientele
  - Topics per importance
  - Customization of storyboards
- Develop the communication strategy and tools:
  - Communication plan
    - Calendar of events
    - Tools
    - Messages

terranova

Assessment

STAGE 1

PLAN

- Measure propensity for secure behavior
  - Protecting passwords
  - Sending sensitive information
  - Avoiding phishing scams
  - Clean desk policy
  - Physically securing laptops
  - Knowledge of internal policies
  - Perception of risks
  - Etc.

terranova

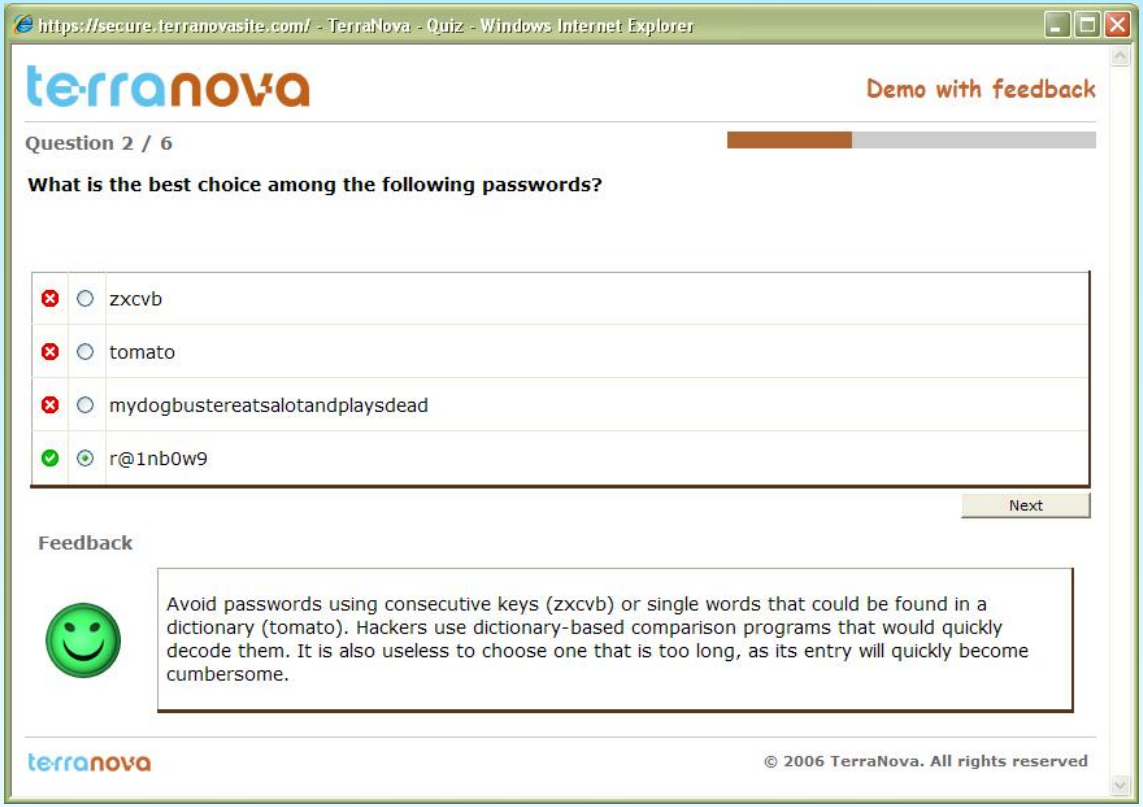
Quiz

STAGE 1

PLAN

Assessment tool

- Evaluates user knowledge level in information security best practices related to human risks and identify weaknesses
- Used as training pre-test and post-test



terranova

Awareness strategies

STAGE 1 **PLAN**

Training

- Executive seminars
- Base line training per clientele
- Videos and reminders

Marketing material and communications

- Key messages based on best practices
- Branding to create rapport
- Posters, wallpaper, etc.

Informational resources: Create space for information sharing

- Intranet space dedicated to security awareness
- Newsletters
- Deliver weekly messages
- Publications

Incentive mechanisms

- Rewards

terranova

Deploy

- Find the key stakeholders within the organization to support the project
- Deploy a communication strategy
- Roll-out training that meets the objectives of the company's security policies

terranova

Start at the top with executive seminars

STAGE 1 → PLAN

STAGE 2 → TRAIN

Make managers one of your delivery channel and get all employees to adhere to security strategy

- What is information security?
- Why is it necessary?
- Responsibilities
- Information classification
- Identifying the threats
- Calculating the risk
- Security measures
- Security policies
- How will we increase information security in our organization

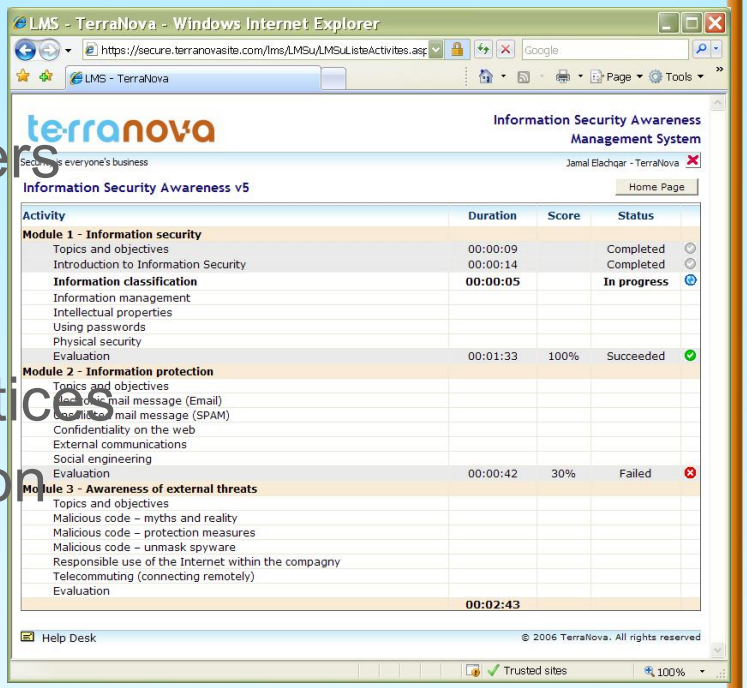
terranova

Security Awareness On-line training

STAGE 1 → **PLAN**

STAGE 2 → **TRAIN**

- Scenario based activities teach users to apply policies
- COTS helps keep costs down
- Key messages based on best practices
- Repeating testing improves retention
- Branding to create rapport
- 60 to 75 minutes of training



terranova

On-line training

- *Introduction*
- Learning Activity
- Conclusion

terranova

Marketing material

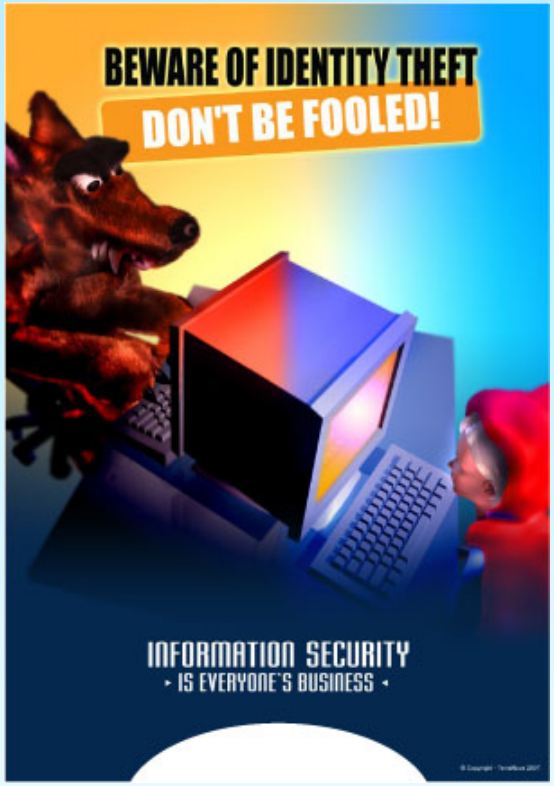
Ensure adequate communications before, during and after training program deployment

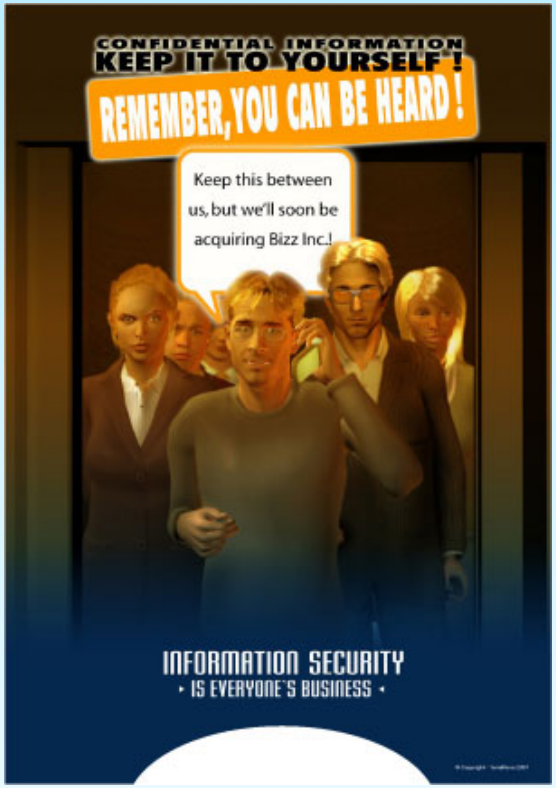
Marketing material

- Slogan: ex: Security is everyone's business
- Posters, ad banners, screen savers
  - To provide fun and motivating tools
  - Keep messages simple and direct
  - Key messages based on best security practices used in every day life
  - Use branding to create rapport

terranova

Posters





terranova

Ad banner

terranova

Comic Strips

terranova

Reinforce

Post-training tool designed to maintain security awareness interest throughout the year

- Corporate Intranet
  - Awareness tips
- Newsletters
- Games

terranova

Assess

- **Training:**
  - Assess & Continuously Measure
    - Percentage of users who have completed the training with success
    - Measure the effectiveness of the project and incorporate changes.
      - Post Assessment quiz
- **Behavior changes (examples)**
  - Data protection: number of documents found unattended
  - Network security: number of time logouts
  - Clean desk policy:% of noncompliance
  - Device security: number of laptops thefts reported

terranova

Maintain & Review

- Once initial training has been introduced and completed you need to maintain the knowledge and increase it continuously as new threats and new best practices are released.
  - Yearly updates of the material

terranova

Thank you

Any questions?

www.tnsecurityawareness.com

terranova