

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

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.

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.



The Project Factor

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

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.

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 (MITR, PCI, SOX?)
4. What are the company's security policies and how are they translated into daily activities?

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.

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.

Baseline and Content Considerations

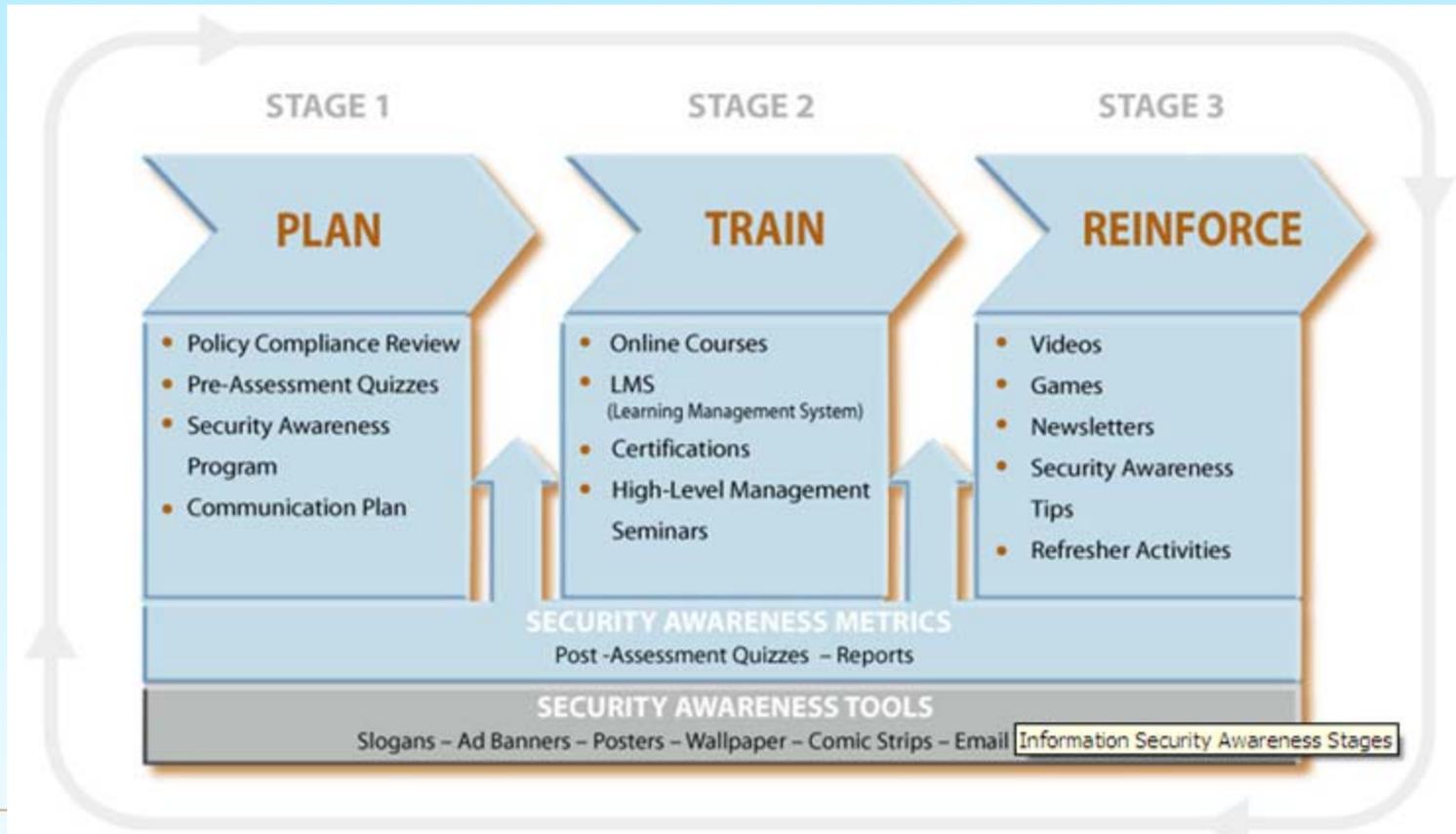
- Use internal security policies and guidelines as well as best practice guidelines
- Establish a baseline of knowledge
- NIST provides some good guidelines (NIST SP 800-50) which include:
 - Recent incidents
 - Regulatory issues
 - Employee concerns
 - Management concerns
 - Customer concerns

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.

Our Approach

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



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

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.

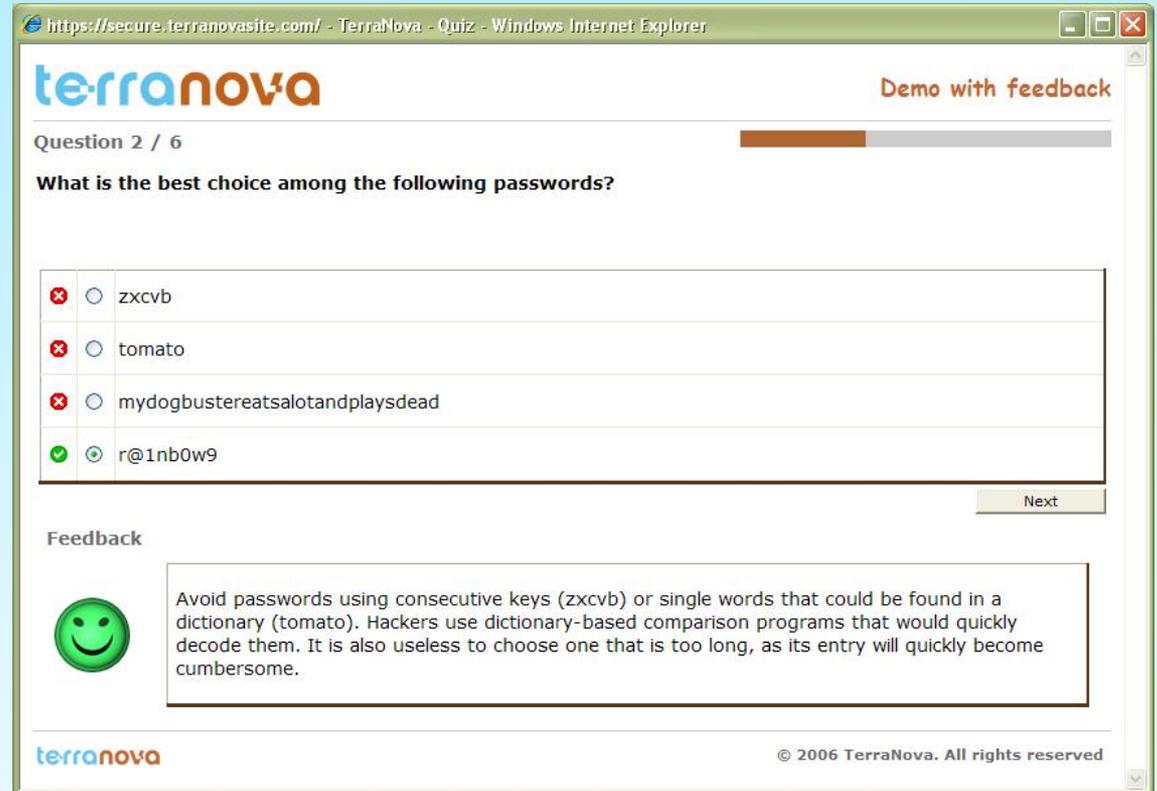
Quiz

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



https://secure.terrannotasite.com/ - TerraNova - Quiz - Windows Internet Explorer

terrannota Demo with feedback

Question 2 / 6

What is the best choice among the following passwords?

- zxcvb
- tomato
- mydogbustereatsalotandplaysdead
- r@1nb0w9

Next

Feedback

 Avoid passwords using consecutive keys (zxcvb) or single words that could be found in a dictionary (tomato). Hackers use dictionary-based comparison programs that would quickly decode them. It is also useless to choose one that is too long, as its entry will quickly become cumbersome.

terrannota © 2006 TerraNova. All rights reserved

terrannota

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

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

Start at the top with executive seminars



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

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

The screenshot shows a web browser window titled "LMS - TerraNova - Windows Internet Explorer" displaying the "Information Security Awareness Management System" interface. The page title is "Information Security Awareness v5". Below the title is a table with columns for "Activity", "Duration", "Score", and "Status".

Activity	Duration	Score	Status
Module 1 - Information security			
Topics and objectives	00:00:09		Completed
Introduction to Information Security	00:00:14		Completed
Information classification	00:00:05		In progress
Information management			
Intellectual properties			
Using passwords			
Physical security			
Evaluation	00:01:33	100%	Succeeded
Module 2 - Information protection			
Topics and objectives			
Confidentiality of email message (Email)			
Confidentiality of email message (SPAM)			
Confidentiality on the web			
External communications			
Social engineering			
Evaluation	00:00:42	30%	Failed
Module 3 - Awareness of external threats			
Topics and objectives			
Malicious code - myths and reality			
Malicious code - protection measures			
Malicious code - unmask spyware			
Responsible use of the Internet within the company			
Telecommuting (connecting remotely)			
Evaluation	00:02:43		

At the bottom of the page, there is a footer that reads "© 2006 TerraNova. All rights reserved." and a "Help Desk" link.

terranova

On-line training

▶ *Introduction*

▶ Learning Activity

▶ Conclusion



The screenshot shows a web browser window with the address bar displaying "https://secure.terranovasite.com/ - Malicious Code - Protection Measures - Introduction - Windows Internet Explorer". The page title is "MALICIOUS CODE - PROTECTION MEASURES". The main content area is titled "INTRODUCTION" and features an illustration of a hand pointing at a tablet. The text reads: "Evidently viruses and other malicious programs are at the head of the list of computer threats. Viruses, worms and Trojan horses are considered malicious programs because they can cause damage to your computer and the data that is saved on it, slow down Internet access and use your computer to infect other computers on a local network or on the Internet. A few preventive measures and good judgment will decrease the probability of your becoming a victim to these threats." Below this text are three buttons labeled "Viruses", "Worms", and "Trojan Horse", each with a magnifying glass icon. At the bottom of the page, there are navigation links for "AUDIO", "GLOSSARY", "QUIT", and "NEXT PAGE". The footer contains the slogan "INFORMATION SECURITY IT'S EVERYONE'S BUSINESS" and copyright information for TerraNova Training Inc. (© 2003-2008) with a logo.

Marketing material

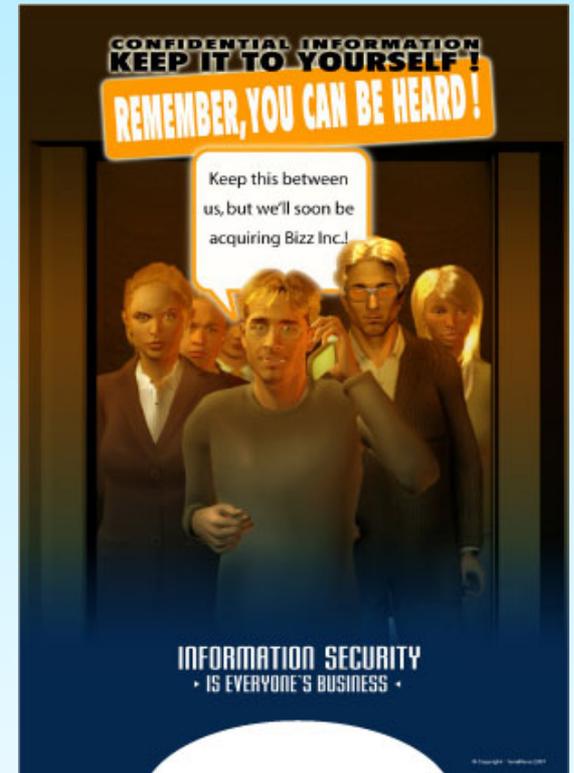
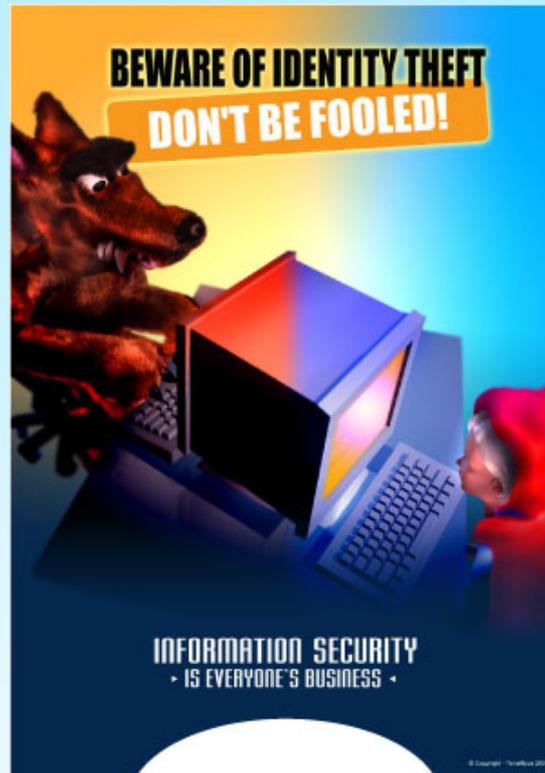
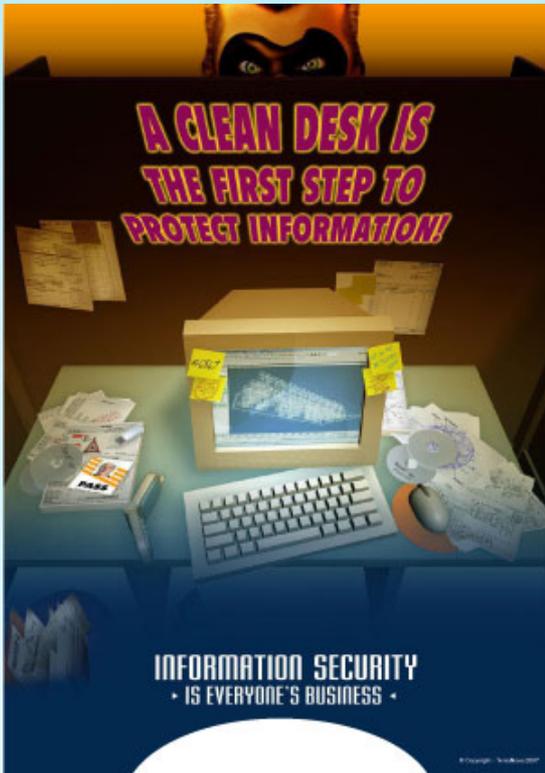


Ensure adequate communications before, during and after training program deployment

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

Posters



Ad banner



terrano

Comic Strips



Reinforce

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

- ▶ Corporate Intranet
 - ▶ Awareness tips
- ▶ Newsletters
- ▶ Games

NEWSLETTER SECURiNFO by terranova

PROTECTION OF PERSONAL INFORMATION

To do

- As an individual, check an organization's policy on the protection of personal information before sharing any such information with it.
- As a manager, appoint someone within your organization to ensure existing laws are respected.

To avoid

- Sharing personal information with business partners.
- Using personal information for purposes other than those for which they were obtained.
- Obtaining personal information under false pretenses.
- Obtaining additional personal information while gathering data.

Consequences

For an organization, failing to adequately protect its customer personal information may expose it to serious consequences:

- Damage to reputation and corporate image;
- Legal action against the organization;
- Loss of trust of clients, employees and business partners;
- Financial losses or lost customers;
- Customers' refusal to provide any personal information;
- Allegations of deceptive marketing practices.

Use personal information only for authorized purposes.

How you go, Regis. No complete members list taken from my database. Will be very useful for your Link-Logos fundraise.

© 2010 Terranova Inc. All rights reserved. This document is confidential and intended solely for the individual named. If you are not the named individual, you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake. Contact us immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system.

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

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

Thank you

Any questions?

www.tnsecurityawareness.com

terrano