Creating a Security Culture

Presented by

John Sancenito

February 10, 2017

Overview

- Insider threats and the need for a security culture.
- Implementing a security awareness program.
- Goals of a security awareness program and obstacles to overcome.
- Key elements of a security awareness program
  - Embedded Security Principles
  - Awareness Training
  - Communication / Reinforcement
  - Empowerment
  - Management Support

INA
Investigate • Protect • Secure

Defining Culture

Culture

"the set of shared attitudes, values, goals, and practices that characterizes an institution or organization"

- Mariam–Webster Dictionary

Security Culture

"the ideas, customs and social behaviors of a group of people, that impacts their security…a subset of the larger cultural scope of any particular people or group"

- Wikipedia

INA
Investigate • Protect • Secure

Have You or Your Staff Ever…

- Loaned a co-worker keys or badges?
- Shared network passwords?
- Propped open an exterior door?
- Left buildings or rooms unlocked?
- Failed to report suspicious activity?
- Provided confidential information over the phone?
- Clicked on a link or email attachment from an unknown source?
- Plugged in a USB drive they found?

INA
Investigate • Protect • Secure

Insider Threat Vulnerabilities

- Insiders who are blind to security threats.
- Insiders who do not know or follow countermeasures.
- Insiders who share too much information.
- Supervisors and managers who do not enforce security procedures.
- Poor contracting decisions and oversight.
- Leaders who fail to enact adequate controls, policies and procedures.

Social Engineering

- Psychological manipulation of people into performing actions or divulging confidential information.
- Methods Include
  - Phishing e-mails
  - Email attachments
  - Ransomware
  - Email Spoofing
  - Pre-text calls
  - Watering hole
  - Cybersquatting

INA
Investigate • Protect • Secure

Managing Insider Threats

- Most vulnerabilities created by ignorance, not malicious intent.
  - Do not think anything bad will happen
  - Do not know or follow security countermeasures
  - Do not feel security is their responsibility
- Most people choose convenience over security!

Source: INA

Obstacles to Overcome

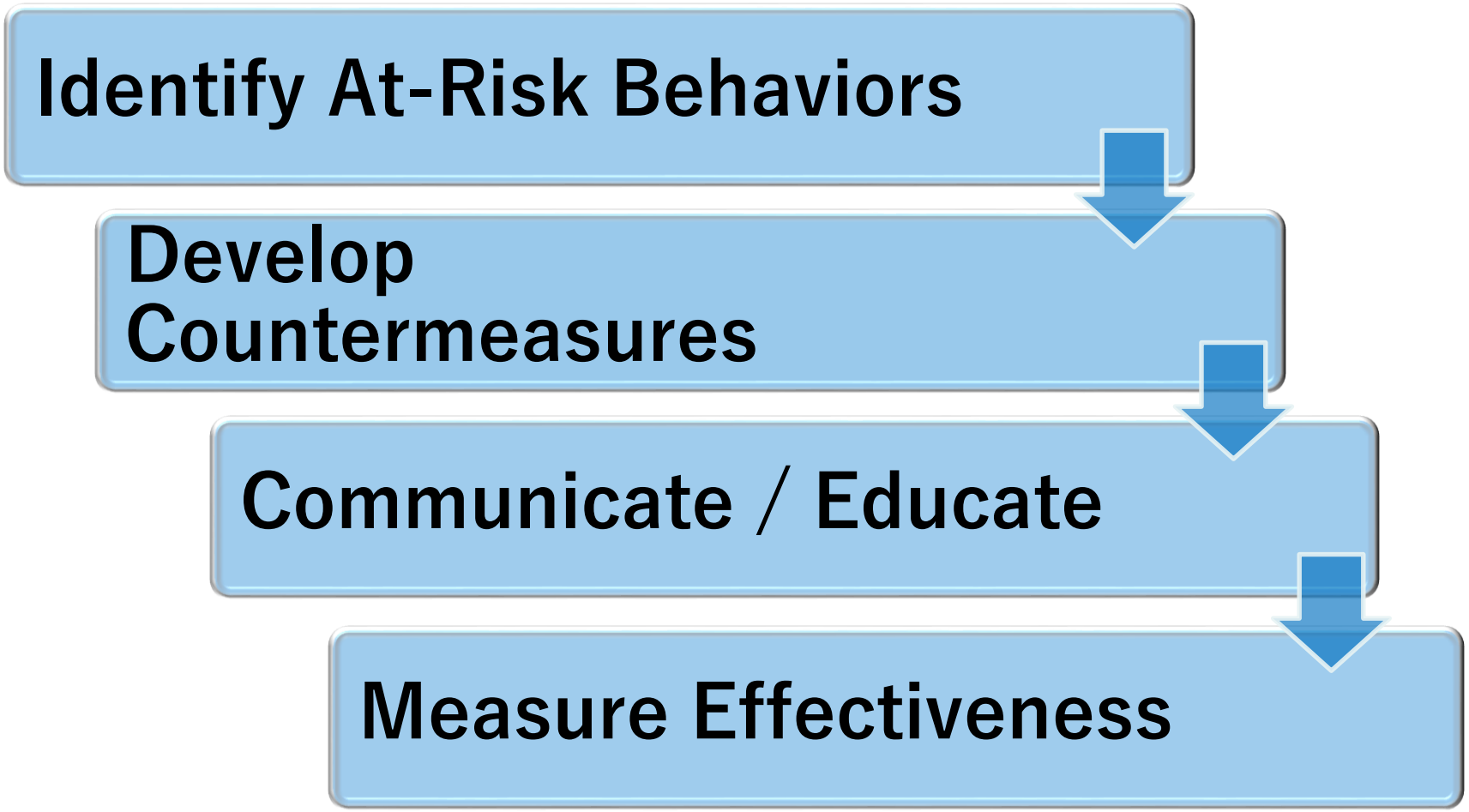
- Resistance to change
- Complacency
- Inconvenience
- Lack of management support
- Lack of long term commitment / resources
- Program buy in / ownership
- Difficulty in measuring value and success
- Poor communication

Goals of a Security Awareness Program

Employees, Visitors and Guests:

- Understand security policies, processes, and procedures.
- Understand their role in maintaining a safe and secure workplace.
- Feel empowered to take an active role in their personal security.
- Increased awareness of surroundings and how to report suspicious activity.
- Reduce fear, panic and dysfunction during an emergency.

Security Awareness Program Process



Key Elements - Security Awareness Program

Embedded Security Principles

Awareness Training

Communication / Reinforcement

Empowerment

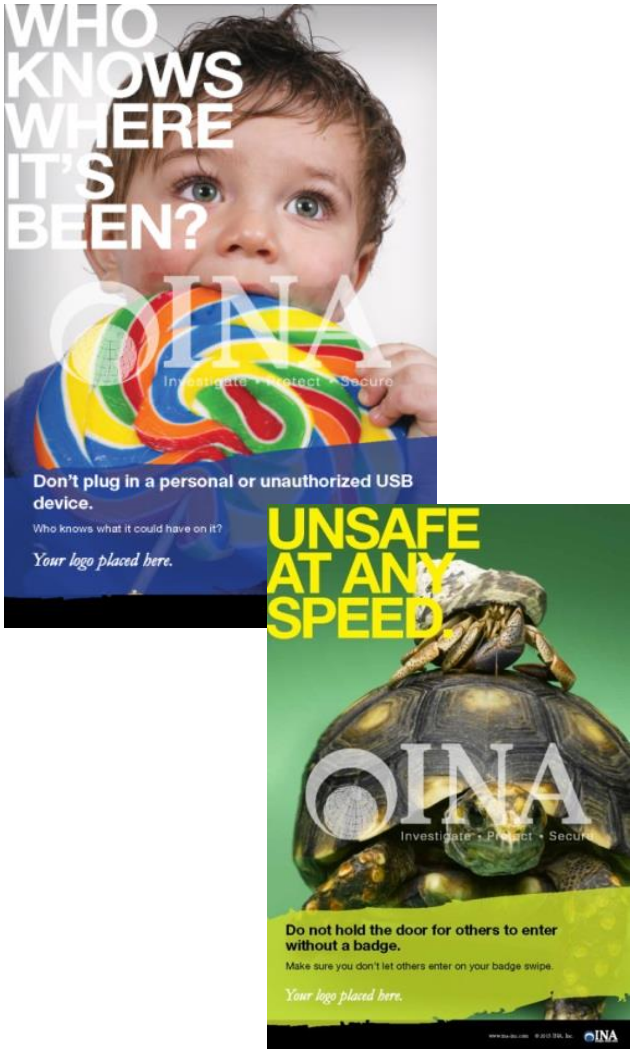
Management Support

Embedded Security Principles

- Include security elements into:
  - Policies
  - Practices
  - SOP's
  - Procedures
- Have systems of checks and balances.
- No one person with absolute control.
- Separate work and private space.

Awareness Training

- Frequency
  - New hire orientation
  - Annually
  - Constant reminders
- Keep it simple, grounded, and behavior focused.
  - Relate to everyday life
  - Use humor
- Reinforce Periodically
  - Posters
  - Email blasts



INA Security Awareness Poster Series © INA

INA
Investigate • Protect • Secure

Security Training Topics

- Access control
  - Propping doors
  - Piggybacking
  - No loaning of badges
- Confidential information
  - Intellectual Property
  - OPSEC / INFOSEC
  - Social engineering scams
  - Phishing
- Suspicious activity
- Challenging strangers
- Data security
  - Email attachments
  - USB Drives
- Following security polices and procedures
- Active Shooter / Hostile Intruder

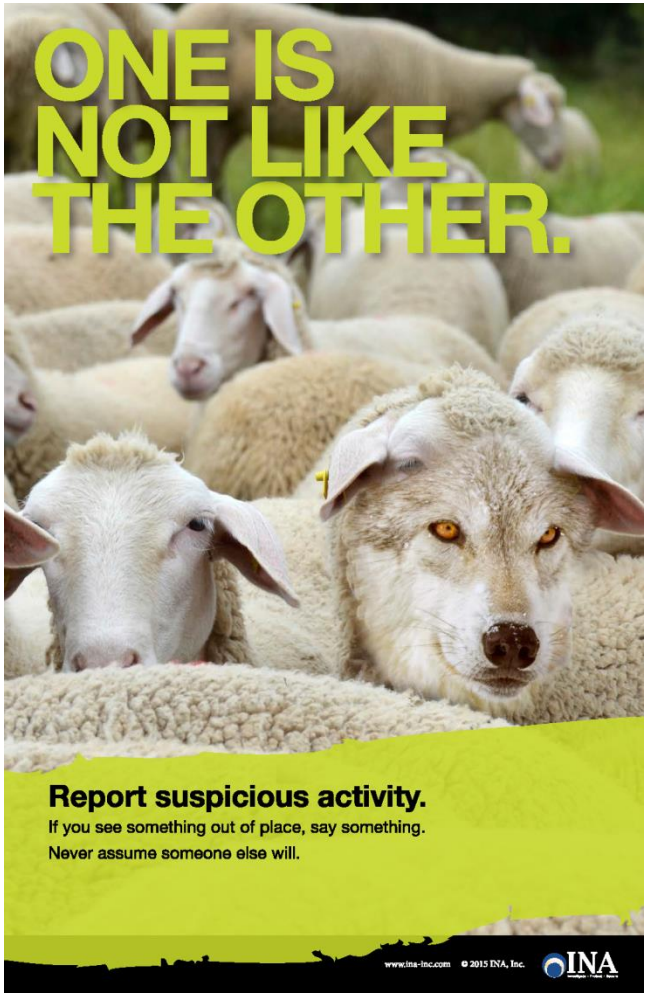
INA
Investigate • Protect • Secure

Communication / Reinforcement

- Create ambassadors or champions to spread security concepts throughout the organization.
- Communicate active threats to employees.
- Let them know what behaviors but them and the organization at risk.
- Periodically reinforce security concepts.
- Make message content engaging:
  - Stories
  - Humor
  - Memorable

INA
Investigate • Protect • Secure

Which is More Effective?



INA
Investigate • Protect • Secure

Empowering Employees

- Atmosphere of personal responsibility.
- Anonymous ethics hotlines.
- Follow up on complaints, issues and concerns.
- Encourage application in everyday life.
- Use positive reinforcement.
- Reward constructive recommendations.

Management Support

- Leadership by example is critical.
- No duel standards.
- Institute adequate compliance and audit procedures.
- Compliance with security programs included in performance evaluations.
- Evaluate supervisors and managers on compliance, not just production.
- Consequences for security violations.

Summary

- Focus on at-risk behaviors.
- Expect resistance to change.
- Recruit ambassadors or champions.
- Set realistic and measureable goals.
- Simple and engaging messages.
- Use different outlets and methods.
- Include visitors and contractors.
- Intertwine security principles in everything you do in your professional and personal life!

INA
Investigate • Protect • Secure

For More Information

John J. Sancenito

President

INA

1-800-443-0824

jsancenito@ina-inc.com

Twitter: #jsancenito

INA
Investigate • Protect • Secure