

New Directions in Security Awareness

Christopher Vera

CISSP, GCFA, GCPA, GLEG

www.mysticnebula.com

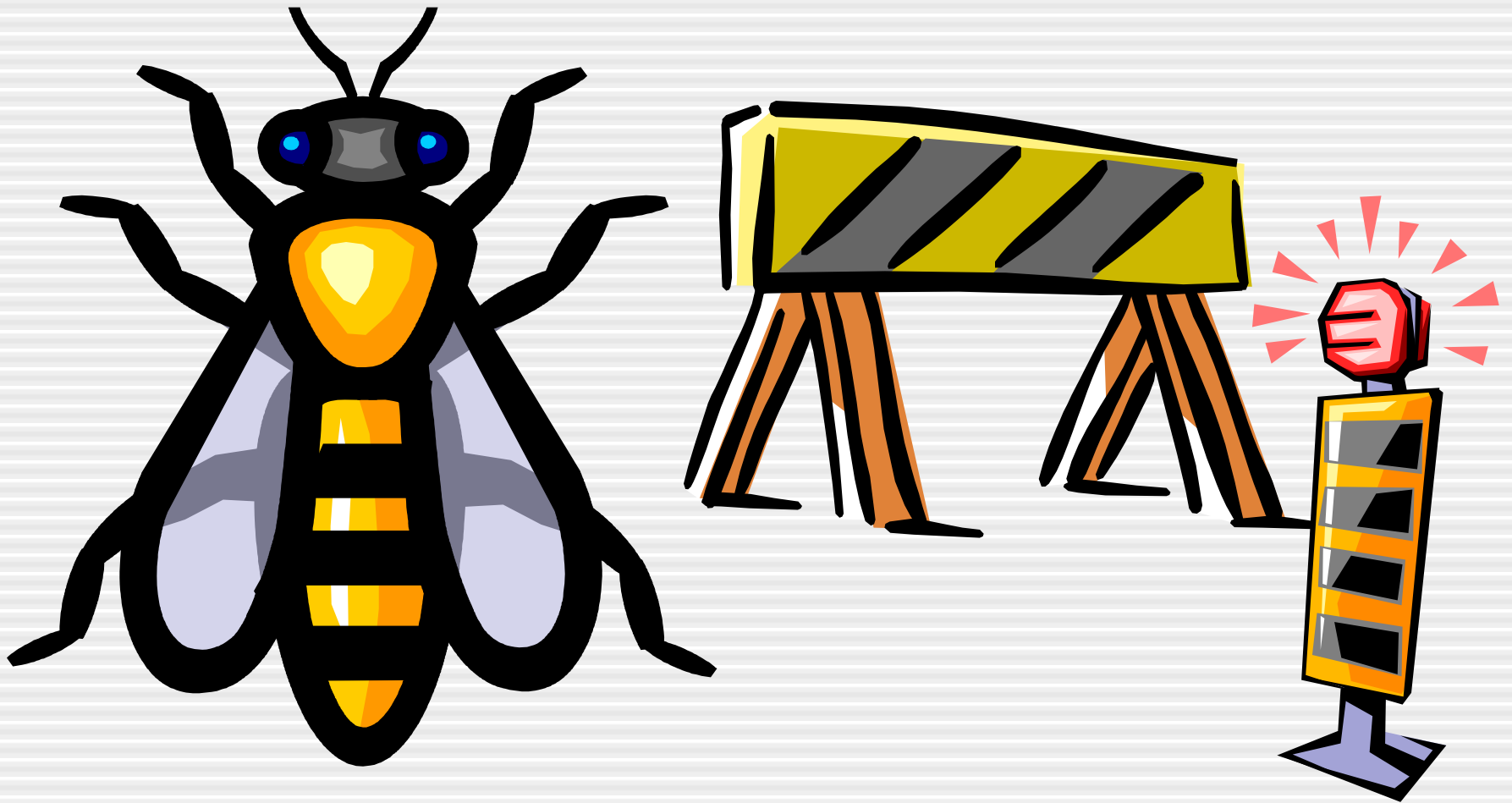
My Experience

- " Security Operations & Awareness Lead
- " Multiple Fortune 500 companies
- " 15,000-45,000 employees
- " Approx. 350 locations in California
- " Other experience
 - Incident Response
 - Vulnerability Management
 - Security Engineering
 - Poetry

My Observations

- " Employees may appear apathetic
 - Lectures
 - Web-Based Trainings
 - Lots of “junk mail”
- " But they consume eagerly when its...
 - Relevant information
 - Provided “just in time”
 - In formats valuable to their jobs

The Power of Awareness



What NIST SP800-50 Says

" Roles & Responsibilities

- Agency Head
- Chief Information Officer
- Security Program Manager
- Managers, Users

" The Continuum

- Awareness > Training > Education

" Design Program

- Structure (Centralized > Decentralized)
- Needs Assessment, Plan
- Priorities, Setting Bar
- Funding

" Developing Program

- Behavior to reinforce
- Skills to learn/apply

" Implementing Program

- Communicating plan
- Delivery techniques

" Post-Implementation

- Monitor Compliance
- Evaluate feedback
- Manage change
- Raise bar
- Success indicators

My Lessons Learned From NIST Model

- " Executive management sponsorship
 - Sponsorship != bobble-head “yes, SA is important”
 - Develop a strong relationship with execs
 - Find ways for execs to play an active role thru life of program
- " Requirements gathering
 - Know the problem(s) you trying to solve
- " Program design
 - Develop vision, strategy
 - Find the right people to lead the program
- " Program implementation
 - Define key objectives
 - Deploy tactics that repeat themes across multiple channels (reinforcement)
- " Maintenance & improvement
 - How will you measure success?

Business Justification

- " ISO 17799 (2000 version)
 - "6.2 User Training"
 - "ensure...users are aware of info security threats & concerns"
- " COBIT
 - "5.0 Train & Educate Users"
- " CA AB1950, Personal Information
 - "implement...reasonable security procedures"
- " PCI Standard
 - "12.6 Implement a formal awareness program..."
- " HIPAA
 - 164.308(a)(5) "Implement a security awareness & training program..."
- " MM 06-12, Protection of Info Assets
 - Applies to CA state agencies
 - "Ongoing education & training..."
- " GLBA
 - 314.4 (b) "...should include... Employee Training"
- " NIST SP800-26 Self Assessment Guide
 - Applies to Federal govt
 - "13.1 Have employees received adequate training...?"
- " NERC CIP
 - Applies to (most) electric utilities
 - "CIP-004 Personnel & Training"

Vision

- " Deliver the right message...
- " To the right people...
- " At the right time

Objectives

" Tactical

- Ensure every employee understands & executes their role according to security policy

" Strategic

- Change culture over time through sustained & consistent behavior modification

Strategy

- " Foundation: Security Policy Framework
 - No consistent security awareness message without it
- " Know Your Business
 - Migrate from security theory into practical application
- " Modularize
 - Make communications multi-purpose & reusable
- " Enlist Security Champions in Business
 - You can't do it alone
 - Champions have respect & knowledge of business
 - Communication is two-way: you learn, they learn
- " Embed Awareness in Business Processes
 - New hire, project lifecycle, procurement, employee evaluations, helpdesks

Ideal SA Lead Candidate

- " Passionate
- " Leader
- " Excellent communicator
 - Written
 - Oral
- " Strategic thinker
- " Able tactician
- " Security experience
 - Important, but notice its at the bottom of my list
 - Broad vs. deep improves versatility

Sales & Marketing 101

- " Security awareness = security sales
 - You're selling life-jackets on a ship the hot sunny day before a big storm
- " Be humble & informative
 - Avoid condescending tone, minimize use of "thou shalt..." & "because its policy"
 - Policy framework is great foundation but terrible for quoting
- " Upsell your security department services
 - "Would you like security engineering fries with that policy question shake?"
- " Build relationships - Get out there!
 - Why do vendors always want to meet face-to-face?
- " Build your brand & plaster it everywhere & on everything
- " Act quickly on feedback
 - Nothing gets people involved like being listened to

The Right People

Your audiences

Your Audiences

- " SA is role-based: the more granular the better
- " Goal: deliver messages to smallest, most relevant audience possible
- " Two Primary Role Types
 - Static
 - Dissolving

Static Audiences

- '' Consider static roles defined in policy
 - Users (of information, applications), Managers
 - Information/Application/System Owners
 - System Administrators/Custodians
 - Risk Acceptors (i.e., Executives)
- '' Other relatively static roles
 - Mobile users
 - Users in business-specific critical roles
 - '' Who makes \$\$\$ for your organization?

Dissolving Audiences

- " Appear for a short time & disappear later
 - Specific needs
 - Typically don't require sustained awareness
- " Examples
 - Project teams
 - Policy violation fire starters
 - Visitors, contractors, consultants

The Right Message

What they need to know

Topic Format Always Same

- " Subject matter is infinite, but
- " Topic always tends to look like this
 - Threat, how to recognize it
 - Impact, what happens if threat materializes
 - How organization expects one to avoid it
 - What to do if one fails to avoid it
- " Emphasis of each section may change, depending on message

Where Do Topics Come From?

- " Trick question: Short answer is EVERYWHERE!
- " Some examples
 - Security Policy Framework
 - News media (often to set the story straight)
 - Incident Response & Monitoring
 - " Policy violations
 - " Incidents related to poor behavior
 - Vulnerability Management
 - " System configuration reports
 - Managers
 - " Managers are the sergeants of your organization, ignore them at your peril
 - Executives
 - " Executive questions make great topics (because you can name drop)

The Right Time

Delivered just before they need it

Communication Workhorses

- " E-mail
- " Web-Based Training
- " Posters
- " Website
- " News articles
- " Zzzzz...not sexy, but how most organizations communicate, take advantage!

Security Blogs

- " Gives security team a place to sound off
 - Keeps them talking about their passion
 - Satisfies role-based audiences
- " Faster to update than average website
- " Allows better content control (unlike e-mail)
 - Correct mistakes quickly
 - Frequent refresh for breaking news
 - Searchable, archive-able
 - Gives audiences a place to respond or ask questions
- " Easy Real Simple Syndication (RSS)
 - Many browsers, Outlook 2007
 - Reduces "junk mail"

Manager Security Bulletins

- " Presents one topic in 3-7 simple bullets
- " Targeted at managers/supervisors
- " Standard format, easy to put together
- " Includes SA program "branding & advertising"
- " Used by managers
 - As posters
 - As staff meeting hand-outs
 - To satisfy departmental awareness requirements

Desktop Alert Tool

- " RSS-like feed in workstation systray
 - Based on SANS ISC Infocon
 - Blog backend
 - Tool polls blog periodically for updates
 - Role-based (users select msgs to receive)
 - Change color of systray icon based on threat level for msgs user cares about
 - Also includes handy right-click links to commonly used resources

Surgical Strike

" Used to

- Stop fires before they get out of control
- Modify behavior in a specific dept or location

" Characterized by

- Shock & awe: rapidly deployed communications
 - " Bulletins, e-mail, staff meetings, screensavers, reports to executives
- Usually more imperative tone

Other Communication Ideas

- '' Promotional Items (never “trinkets”)
 - Keep them office practical (pens, post-its, etc.)
 - Include branding & awareness message
- '' Tradeshow Exhibit
 - All-hands meetings, company rallies
- '' Magazine Subscriptions
 - Targeted employees (i.e., executives, etc.)
 - Technical staff breakrooms
 - Common conference rooms

Even More Ideas

- " Executives ARE communications vehicles
 - Use executives to deliver specific messages
- " Embedded awareness in other communications
 - E-mail quarantine summary (for junk mail)
 - Logon pages of applications
 - “Welcome...” messages when user signs up for new service

What About Metrics?

“Past performance doesn’t guarantee future success”

- ” Problem: What can SA program take full credit for?
 - Reduced Incident count? (SA or newly deployed IPS?)
 - Better passwords? (SA or recent change to complexity rules?)
- ” Solution: Look for soft metrics that indicate culture change
 - More frequent contacts from “human IDS”
 - More frequent requests for help or info
 - Other people delivering relevant security content on their own
 - Risk Acceptors budgeting security \$\$\$ in projects
 - Info & system owners proactively securing their assets

Five Stages of Security Enlightenment*

" Denial

- "Its never happened to us before!"

" Anger

- "Why do I have to do this?! No one else is!"

" Bargaining

- "Look, I'll meet requirement X if I can skip Y & Z."

" Depression

- "I don't care anymore, my project's behind schedule."

" Acceptance

- "I'll do what it takes to satisfy security policy."

(* modified from Rich Bryan & Kubler-Ross Stages of Grief)