WALSH SM COLLEGE

The power to succeed.

Total Security Awareness Training

Who, What, When, Why, How

Nan Poulios

Director IAC

March 2006

Who's Viewing Your Data?

http://www.nbc10.com/money/3975070/detail.html

Agenda

- Why is awareness training important?
- Meeting Requirements
- Getting Started
- Critical Success Factors
- Challenges
- Retention
- Effective Measures and Outcomes

Don’t Let Your Name Appear

The power to succeed.

WALSH COLLEGE

Wells Fargo

- Nov, 2003 – 200,000 names, Credit Card #'s, SS #'s stolen during break-in and theft of contractor laptop
- Feb. 26, 2004 – rental car stolen from gas station with laptop in trunk, contained over 1000 names, addresses, SS #'s of mortgage customers
- http://www.identitytheft911.com/education/articles/art20040416wells.htm

The Register

An Israeli couple faces prison after confessing to the development and sale of a spyware Trojan horse that helped private investigators snoop on their clients' business competitors.

Ruth Brier-Haephrati, 28, and Michael Haephrati, 44, have entered guilty pleas to industrial espionage charges over the Trojan horse case. Ruth was charged with a litany of offences including fraud, planting computer viruses, and conspiracy. Her husband, Michael, is charged with aiding and abetting those offences, Ha'aretz reports. Ruth faces four years in jail while Michael faces two years' imprisonment. Each also faces a suspended sentence and a fine of one million New Israeli Shekels ($212K) under a plea-bargaining agreement. Tel Aviv District Court Judge Bracha Ofir-Tom will rule on whether the Haephrati's plea is acceptable on 27 March.

http://www.theregister.co.uk/2006/03/15/spyware_trojan_guilty_plea/

BJ's

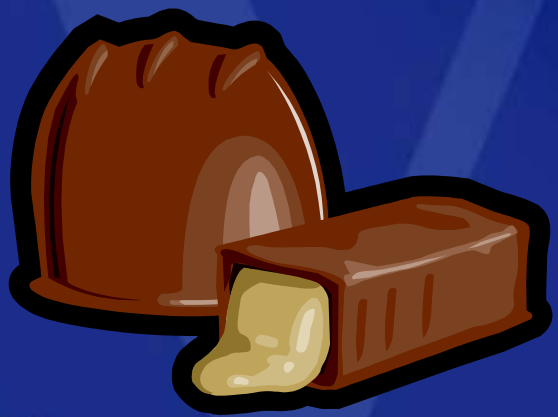
- March, 2004 - Theft of computerized credit card data from warehouse club
- Faces lawsuits from 12 banks for replacement costs of hundreds of thousands of Credit Cards and reimbursement of fraudulent activity

- http://business.bostonherald.com/technologyNews/view.bg?articleid=34432&format=

High Employee Expectations?

A survey of office workers at Liverpool Street Station found that 71% were willing to part with their password for a chocolate bar.

-- Infosecurity Europe 2004




DON'T LET SPAM BOG YOU DOWN.
DELETE SUSPICIOUS EMAIL!
SPAM

Gray Hat Report*

- Researches downloaded viruses, worms, spyware, malware, bots etc.
- Used 179 antivirus, spyware blockers etc. against the infected drive
- Results??
- **Only identified and cleaned 80% of malware.**

**Gary Hat Presentation to Detroit ISACA 3-15-06*

Regulatory Requirements

Yes, there are requirements!

Training Requirements

- ISO 17799 6.2.1 Information security education and training All employees of the organization and, where relevant, third party users, should receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages, before access to information or services is granted.

- FFIEC Examiner's Handbook, "Security Controls Implementation: PERSONNEL SECURITY: states, "Financial institutions should mitigate the risks posed by internal users by providing training to support awareness and policy compliance."

- NCUA 748 Appendix A III (B) 2. Train staff to implement the credit union's information security program.

Training Requirements 2

- Safeguards Rule § 314.4 Elements."(1) Employee training and management;"

- Cobit 7.0 Manage Human Resources 7.4
  1. Management should ensure that employees are provided with orientation upon hiring and
  2. with on-going training to maintain their knowledge, skills, abilities and security awareness to
  3. the level required to perform effectively.
  4. Education and training programs conducted to effectively raise the technical and management skill levels of personnel should be reviewed
  5. regularly.

Training Requirements 3

- NERC 1200: "The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function shall train personnel commensurate with their access to critical cyber assets. The training shall address, at a minimum: the cyber security policy, physical and electronic access controls to critical cyber assets, the release of critical cyber asset information, potential threat incident reporting, and action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident. Training shall be conducted upon initial employment and reviewed annually."

Training Requirements 4

- FISMA **§ 3544. Federal agency responsibilities**
- ‘‘(4) security awareness training to inform personnel,
- including contractors and other users of information systems
- that support the operations and assets of the agency, of—
- ‘‘(A) information security risks associated with their
- activities; and
- ‘‘(B) their responsibilities in complying with agency
- policies and procedures designed to reduce these risks;’’

Training Requirements 5

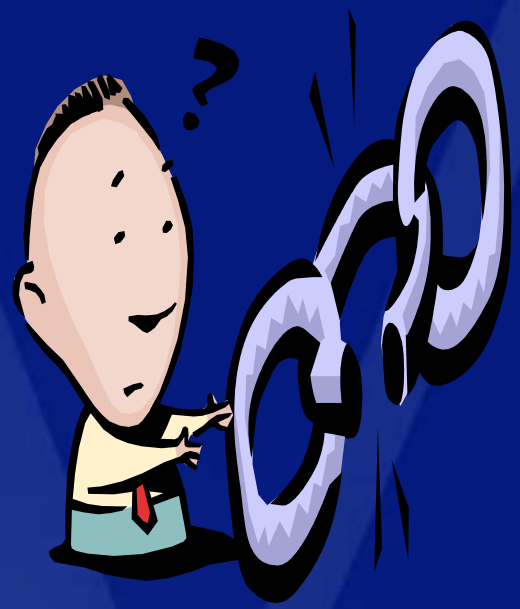
- Department of Homeland Security – 21 Steps for Securing SCADA
  - "People can be a weak link in an otherwise secure network.
  - Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords."

Key Challenges

- Systems alone are not enough
- Overcoming complacency
- Different target audiences
- Delivering the program
  - Ongoing program
  - Cost-effective
  - Creative and engaging activities
- Measuring the results
- Demonstrating compliance

Target Audience Challenges

- Management
- Technical Staff
- Developers
- End-users



What Does It Mean to Me?

- Training scenarios must make sense to the audience
- Training scenarios must be relevant to daily tasks
- Ideas??
  - Normal user
  - Manager
  - Developer
  - Network Engineer/architect

Now Teach the Safeguard

- Gain understanding of threat and their behavior
- Understand the importance of compliance with your security program
- Increase retention

Ultimate Goal

- Bringing about meaningful behavior change
- Not just passing a quiz or signing a policy statement
- On-going protection of assets

Getting Started

More than Buying a Program

Common Mistakes

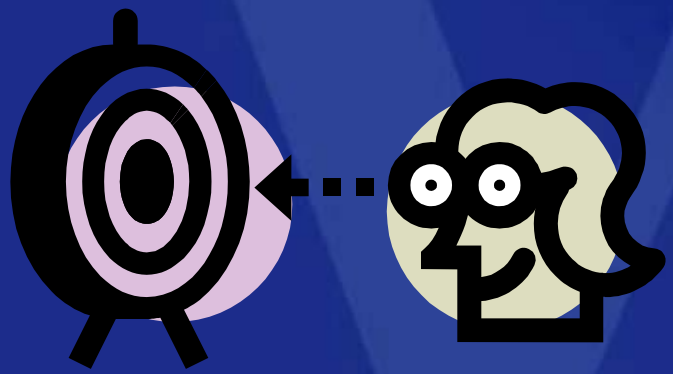
- Publishing policy won't meet your goals for behavioral change
- Not partnering with your Training Department – IS Manager is not a training professional
- Once a year training is not enough
- Static presentations are not effective learning tools

You Need a Team

- Project Manager
- SME's
- Business Representative
- Training Representative
- Technical Representative

Training Needs Analysis

- Assesses current level of awareness
- Evaluate current environment
- Identify target audiences
- Define training/learning objectives



Critical Success Factors

- Meet needs of target audience – non-technical vs. technical
- Custom Content? Do you have the resources?
- Media and delivery channels
- Cultural factors
- Languages
- Timeframes
- Support or help desk

Critical Success Factors

- Current Status Audit
  - Current Infrastructure
  - Desktop Configuration
  - Bandwidth
  - Existing LMS delivery tool
  - SCORM compliant
  - Section 508

Critical Success Factors

Project planning

- Develop an overall communications plan
  - e-learning is just one component
  - Communicate with and gain buy-in from senior management
- Plan beyond initial training
- Include technology and integration requirements
- Clearly defined roles and responsibilities
- Agreed *realistic* timescales and clear milestones
- Regular reporting and reviews

Developing the Training

What is Right for You?

What is Best?

Depends on You!

- Learning objectives
- Size or number to be trained
- Budget
- Internal resources
- Management support

Awareness Campaign

- Marketing Kickoff
- Core training
- Refresher training/awareness
- Ongoing awareness/Internal Marketing

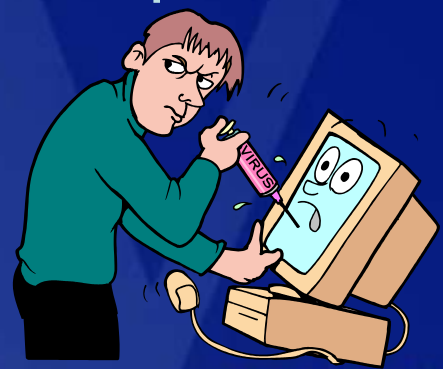
Rules of Engagement

When conducting activities

1. No names – non-punitive
2. Establish Rules
3. Publish winning results
    1. Staff newsletter
    2. E-mail
    3. Wall of Winners
4. Hand-out awards
    1. Poster for cubicle
    2. Extra afternoon or day off
    3. Gift Certificate
    4. Security Token
    5. Gift Certificate
    6. Pizza Party for Department

Interactive Training Activities

- General Cyber Awareness
  - Personal Protection – lunch and learn
  - http://iacmembers.walshcollege.edu:8080/
  - ID theft - lunch and learn
  - How to Protect you personal computer from Malware – lunch and learn
- Make these interactive



Interactive Training Activities 2

- Use a Training Lab or personal laptops
  - Install and run free spyware blockers and train on home use
  - On lab PCs install free password crackers
  - Train home users on MS firewall or free Zone Alarm FW
  - Detail Security Settings in MS XP OS
  - Have users search the Internet for their own or their family member's personal information

Interactive Training Activities 3

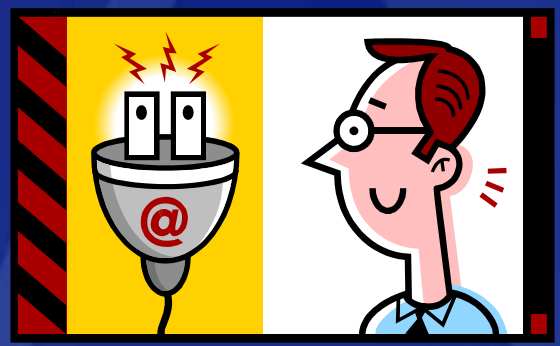
- Have attendees download WinPCAP and Ethereal
- Enter into an IM session with a friend
- Sniff the sessions and review the files.
- This shocks many attendees!

Interactive Training Activities Office

- Have attendees sign in on a PC loaded with a keystroke logger and password cracker
- Run the cracker during the training session
- When attendees feel confident that they used a strong password that wasn't cracked:
  - Open you e-mail and show the key logger results!

Interactive Training Activities 3

- Cookie Poisoning
- SQL Injections
- GPG
- Be creative with screen shots for online learning!



Interactive Training Activities Physical Security

- Piggy Back Fun
  - Have selected staff members try to piggy-back into the facility
  - Record results
  - Award individuals or departments who didn't allow anyone to piggy back

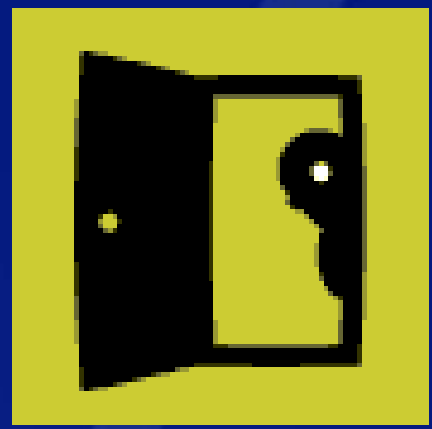
Policy Question of the Month

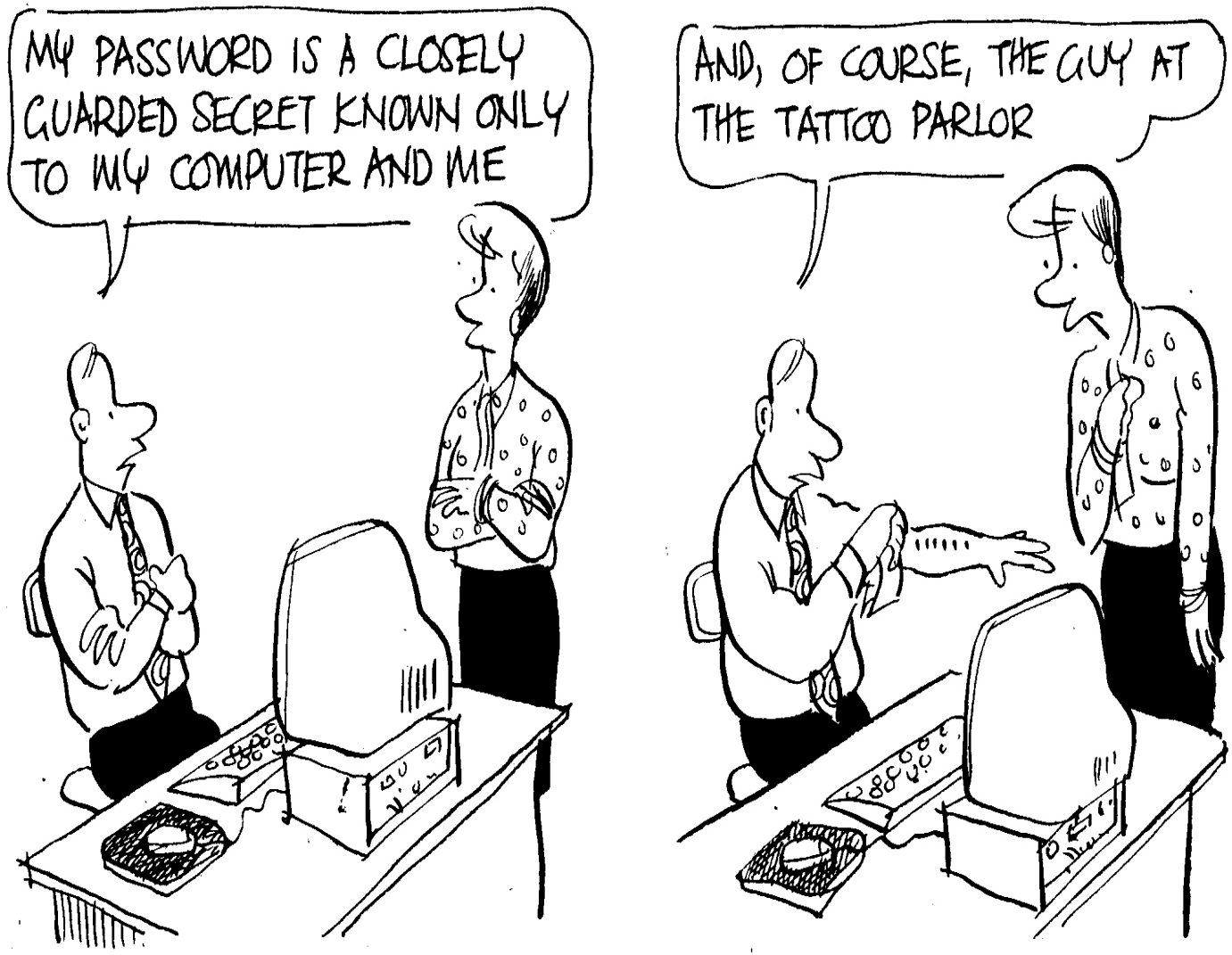
- Send a policy question to each department
- Reward the department with the most correct answers

National Security Agency

Office Walk Through

- Various policy compliance activities may be assessed
  - Screen savers
  - Clean desk
  - Locked desks, file cabinets
  - PC's turned off
  - Modems turned off
  - Entrances propped open for smokers
  - Help carrying out equipment





Newsletters – vary the format of the message

Evaluation and Measurement

Building Success

What Measurements?

- Audit and track attendees
- Track time
- Quizzes
- Evaluations

Type of Measurement

- Track completion
- Evaluate training program (opinion)
- Track understanding pre and post training
- Track retention rate
- Knowledge based test
- Behavioral change performance based

Baseline

- Measure Improvement
- Start with questionnaire before training
- Measure again after training

Knowledge Based

- Quiz
- Test
- Game

Behavior Change

- Ultimate Goal
- Measure performance
- Password cracking example
- Calls to help desk
- Monitor incidents such as virus infections, loading unapproved software
- Remember to baseline


Questions?
The power to succeed.
WALSH SM COLLEGE

Thank You

Nan Poulios

npoulios@walshcollege.edu

248-823-1369