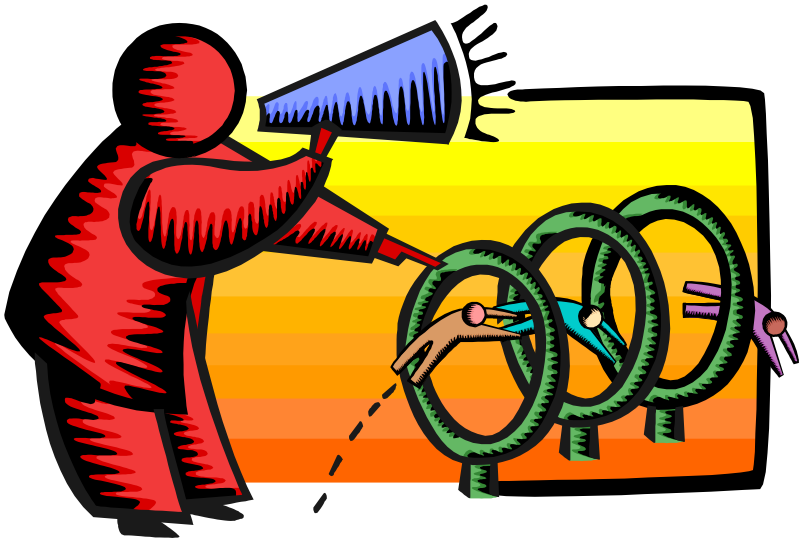
Information Security Awareness

The 6 Cent Model:
Securing Resources

Joe Bower (908) 203-2760
joseph.bower@us.hsbc.com

The Six Cent Model: Agenda

- Setting the Stage
- Sizing the Opportunity
- Message vs. Method
- Meeting the Sponsor
- Seizing the Opportunity
- Summary
- Questions



Two Approaches

- **Funding Based on Design**
- **Design Based on Funding**

The Six Cent Model: Setting the Stage

- **Know Your Topic**
  - You're in Sales
  - Benefits of SA
- **Know Your Audience**
  - For the sale
  - For the program
  - Funding level constrains both the audience and the offering
- **Know The Methods**
  - Cost
  - Logistics
  - Benefits
- **Know Your Purpose**
  - Define scope
  - Define objectives
  - Measured by . . .
  - Required by . . .
  - Partners
  - Risk of not providing
- **Know Your Goal**
  - Get funded
  - At any level
  - Defined expectations

The Six Cent Model: Setting the Stage - Benefits of SA

- Protect Organization
  - Assets
  - Reputation
- Demonstrate strategic intent
- Motivate staff
  - employees
  - vendors
  - consultants
- Reduce cost and time to market
- Tangible proof to customers
- Due Diligence
- Business advantage
- Knowledge leads to actions
- Specific knowledge for specific risks
- Facilitate consistent disciplinary action
- Improve consistency and effectiveness of current controls
- Improve compliance to Standards
- Improve compliance to regulatory and third party requirements

Two perspectives

- **Low head count - total price**
- **Large head count - unit price**

The Six Cent Model: Sizing the Opportunity

3. How many employees, consultants and interns are in your organization? (Choose one)

a. Less than 500

28.9% (24)

b. 501 to 1,000

3.6% (3)

c. 1,001 to 2,500

4.8% (4)

d. 2,501 to 5,000

7.2% (6)

e. More than 5,000

54.2% (45)

The Six Cent Model: Sizing the Opportunity

2. If you have an information security awareness program what is the cost per employee? (Choose One)

a. $0 to $50

34.9% (29)

b. $51 to $75

7.2% (6)

c. $76 to $100

1.2% (1)

d. More than $100

2.4% (2)

e. N/A

10.8% (9)

f. Don't Know

41% (34)

Simple Formula:

Staff count X Days X $ Cost = Funding (Yr/person)

300 x 260 x .25 = $19,500 ($65)

500 X 260 X .20 = $ 26,000 ($52)

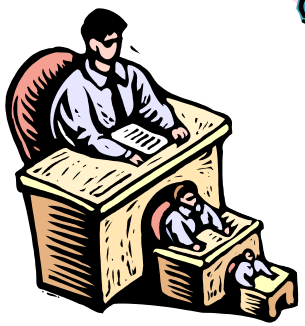
1,000 X 260 X .10 = $26,000 ($26)

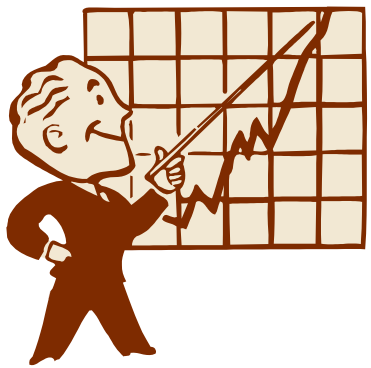
10,000 X 260 X .10 = $260,000 ($26)

55,000 x 260 x .06 = $858,000 ($15.60)

(exclusive of travel and head count)

The Six Cent Model: Message vs. Method





Message:

What you want to communicate

Method:

How you communicate

Decision:

Funding determines HOW you communicate, not what.

Make the Points Supporting Awareness:

- Benefits of a program, and the risk of loss without a program
- Required by law/regulators
- Customer trust and satisfaction
- Protects organizational reputation
- Makes individuals responsible
  - Most critical step to improve information security
  - Best use of dollars
- Demonstrates due-diligence by Management
  - Lack of funding demonstrates weak management commitment
- Talk in terms that aligns the program with the executive's Goals and Objectives

Make the Points Supporting Awareness:

- **Don’t talk in terms that are important to you: talk in terms that are important to the sponsor!**
- **Know your facts – cold!!!**
- **Keep it simple and concise**
- **Keep it non-technical**
- **Be ready to pivot**
- **Demonstrate value: show what you get for the money**
- **Explain what the executive must do (besides funding)**
- **See Rebecca Herold’s book, *Managing an Information Security and Privacy Awareness and Training Program*, for help with meeting specifics.**
- **Get the commitment! (details can follow)**

The Six Cent Model: Seizing the Opportunity

- **Select the Methods**
  - Use multiple methods when possible
  - Same words, different presentations
- **Adapt message to the Method**
  - Graphics, humor, real-life examples
- **Repeat, repeat, repeat**
  - Spaced repetition is the best learning method
- **Know how to measure effectiveness**
  - Mandatory preferred
  - Culture change over time

The Six Cent Model: Seizing the Opportunity

Access Control

Once inside a facility, HSBC protects information by following strict access control procedures to information systems and data assets.

- Never try to access a system for which you are not authorized.
- Follow department procedures for accessing a system.
- Never give anyone your logon ID and password combination.
- Managers must remove employees from an access list when their work no longer requires access.
- Your access authorizations may change as your job and tasks change.
- When you let someone in a secure area, verify that they have a right to enter the area.
- Keep secure areas secured!
- Do not prop open doors to secure areas.

Data Protection and Privacy

One of HSBC's greatest asset is information: about our business, our consumers, our customers, and our employees. Every employee must protect our information.

- Follow your department procedures for using information systems.
- Accept your responsibility for protecting information.
- Do not give out confidential information. Challenge the request.
- Participate in training courses such as the Anti-money Laundering (AML) course and the Security Awareness program.
- Read the Information Protection Standard (IPS) and know your role. Apply what you learn.
- Only send confidential information using secure transport methods; e.g. encrypted files, tamper proof envelopes.

Confidential Information

- Confidential Company Information includes business plans, partner information, unannounced financial results, organization charts, and network information.
- Confidential Customer Information includes name, address, taxpayer ID, account number and details, credit reports, application details, and personal information.
- Confidential Employee Information includes taxpayer ID, passwords, annual reviews, salary, health records, and any personal statements.

Note: See the IPS for more details.

- Follow the instructions in the Information Protection Agreement.
- Be sure to verify the identity of the person asking for information; e.g. Know Your Customer.
- Be sure the person asking for the information has the Need to Know and the Right to Know.

Passwords

- Never give your password to anyone: not your manager, not Information Security, not the Help Desk.
- If anyone asks for your password, report it as a Security Incident (see REACT section).
- If you write down your password, never write the whole password. Use a code as a memory jogger.
- Use strong passwords: one number, one lowercase and uppercase letter, and one special character.
- Passwords should be at least seven characters long.
- Different systems may have different password formats; e.g. length, usable characters, case sensitive.
- Never leave your password list in an obvious place: under your mouse pad or keyboard, taped to your monitor, on your wall, taped inside a drawer.
- HSBC systems remind you when it is time to change your password.

Workstation, PC, and Laptop Security

- Always lock your workstation when you leave: for breaks, for meetings, leave your desk area at the end of the workday.
- Always keep your data files backed up on a network drive
- When travelling, do not leave your laptop alone.
- In the hotel, keep the laptop out of sight when you leave the room.
- You must not use any personal computing device on HSBC premises.
- You must not use mass storage devices, such as CD-writers, thumb drives, or memory sticks, without specific written approval.
- Never log onto the network, and then let someone else use your PC. You are responsible for all actions when you log onto a PC or workstation.
- You must not add personal software to your PC or workstation. This includes graphics for screen savers.

Virus Protection and Management

A computer virus, worm, or trojan is a file that can cripple your workstation and the HSBC network. HSBC has a number of protections in place to minimize the likelihood of a virus entering our network. You, the user, also have responsibilities to help protect our computing resources.

- Never tamper with your anti-virus software settings.
- Never download freeware, shareware, or other programs from the Internet.
- Never load personal software onto your HSBC computer.
- Never open an e-mail attachment from someone that you do not know.

If you think you have a virus or other problem, call the Help Desk to report it.

The Six Cent Model: Seizing the Opportunity

MOTIVATE OTHERS

- Deliver an effective security motivation program to support the HSBC continuing awareness effort.
- Provide feedback to your staff so that they know when security is improving. Feedback improves compliance and performance.
- Share security measures with your staff. Sharing performance metrics lets your staff know how they are performing and increases program buy-in.
- Encourage specific employees to take on public responsibility for information security within their work groups.
- Tier recognition and recognize ongoing compliance. A goal of security is to sustain normal operations.
- Provide immediate awards and favorable performance reviews to those who consistently comply with security requirements. Immediate recognition has a greater impact. Unexpected recognition is more appreciated. Recognizing ongoing security compliance raises the level of compliance.
- Give tangible awards. Reward with give-away items such as coffee cups, or framed certificates, lunch/dinner certificates, time off, or increased training opportunities.
- Publicize awards. Publicize and reward high training attendance rates.
- Let staff know that security compliance is expected and appreciated.
- Let senior management know when their staff are exceeding expectations.
- Make security a part of every employees' job performance. Let your staff know that following good security practices aids in career advancement.

- Put commendations in personnel files of those with exemplary security behaviors.
- Establish performance metrics. Include measures that allow you to identify abrupt workflow changes (e.g., work errors increase).
- Ensure that your staff has completed awareness training within established time frames.
- Publicize both the carrots and sticks to the point where getting a carrot is something to be sought after and getting a stick is something to be ashamed of. Create pride in good security awareness.

RECOGNIZE AND RESPOND TO POOR SECURITY BEHAVIORS

- Prosecute those who compromise customer data. Your willingness to take legal action to protect customer data increases security's importance.
- Provide training to those who unintentionally fail to comply. The willingness to provide training shows that security is important and that procedures are reasonable.
- Quickly remove those who put customer data at risk from positions of trust. Removing individuals who threaten security lets staff know that actions have consequences and improves compliance.
- Avoid recognizing security performance only after a security failure.
- Publicize sanctions for poor security behaviors. Promote the perception that individuals who compromise customer data will be admonished. This improves compliance and reduces customer complaints.
- Treat failure to act responsibly as a serious matter. Convey clear and meaningful sanctions for failing to act when a security violation is observed to all staff.

- Discuss security failures in staff meetings and request mitigation approaches. Staff buy-in to solutions increases compliance.
- Use sanitized versions of security failure scenarios in training.
- Use behavior correction techniques for minor failures. For example, require remedial training, place staff on probation with increased monitoring, or place a letter in the worker's personnel file.
- Monitor compliance of high- and low- status individuals more closely. Work with these people if the present security culture is poor.
- Use rapid termination for significant or repeated failures. Immediate removal from a trusted position demonstrates concern for protection of customer data and corporate assets.

INCIDENT PREVENTION AND RESPONSE

- Identify the systems needed to support your business functions. Decide what needs to be protected and focus on security measures (e.g., customer data has high priority).
- Document the business workflow to facilitate identification of abnormal activity.
- Establish Standard Operating Procedures (SOPs) for your business functions.
- Use corporate checklists to avoid overlooking critical areas of concern.
- Schedule internal and third party audits of systems and procedures (looking toward improving compliance, not fault-finding).
- Ensure that you have effective separation of duties or increase oversight when effective separation is not possible.
- Establish a procedure for review of abnormal activity for possible security impact.

The Six Cent Model: Summary

- Know WHAT to communicate
- Know HOW to communicate
- Define audience
  - Awareness vs. training vs. education
- Determine preferred funding level
- Build the business case
  - Allies
  - Existing programs (e.g. HR, Training)
  - Know the benefits
- Make the Sale and get funded
- Allocate resources to most-effective methods
- Know how to measure and track effectiveness

Awareness without Action is worse than Ignorance!