

Security Policies and Awareness

Your First Line of Defense

*Central Ohio ISACA Chapter Meeting
May 11, 2006*

*Anne E. Terwilliger, CISSP
Accentuate Security, Inc.*

- **What Is The Greatest Risk To Security Today?**
- **Security Policies**
 - What is a Policy?
 - What a Policy Is NOT
 - Goals
 - Driven By What Threat?
 - Requirements
 - Who Should Write the Policies?
 - Writing the Policy – Format and Content
 - Who Should Review the Policies?
 - Which Body Should Approve Them?
 - Policy Lifecycle

- **Security Awareness**
 - What Is Security Awareness?
 - Why Is Security Awareness So Critical?
 - You Recognize The Need – Now What?
 - What Should You Cover In The Program?
 - How Should You Cover The Material?
 - Security Checklist
 - The Program Is Finished – Or Is It?
 - Get Ready To Start Again

IGNORANCE

- What is a Security Policy?
 - High-level statement from Senior Management on what to do in a given situation
 - Three types of policies are usually written
 - Program Policy
 - » Defines the intent of the information security program
 - » Program's scope within the organization
 - » Assigns responsibilities for implementation
 - » Compliance
 - Issue specific policies
 - Application specific policies

- **Standard**
 - A standard is a technical means of complying with a policy
- **Guideline**
 - A guideline is a suggested action but one that is not required
- **Procedure**
 - Step-by-step directions to accomplish a task

- **Maintain the C I A**
 - **C** onfidentiality
 - **I** ntegrity
 - and
 - **A** vailability

of Information Assets

- Unauthorized
 - Access
 - Modification
 - Disclosure
 - Destruction (whether deliberate or accidental) of the systems and applications that process the information

- Documented where employees can find them
- Communicated to employees and, in some cases, to individuals outside the organization
- Easy to read
- “Do-able”
- Enforceable
- Applicable to your organization
 - Beware of “canned” policies

- Someone who can take technical terminology and place it into layman's language
 - Does not need to be the SME on the topic
 - Needs to document content from the SME on the topic
 - Needs to have a lot of patience with the process

- Format
 - Be consistent throughout
 - Capture the look and feel of your organization
- Content
 - Explain the
 - Who – employee responsibilities and obligations
 - What – topic under discussion
 - Where – the Scope of the policy
 - When – Date policy takes effect
 - How – what to do to be in compliance
 - Why – Reason the policy developed (vulnerability, Federal law, or ?)

- Working group made up of
 - Information security professionals
 - Audit
 - HR
 - Legal
 - Regulatory Risk Management (if a financial institution)
 - Your average user

- Which body approves the policy?
 - Board of Directors?
 - Executive Management?
 - Working Group?

The answer is:

That depends

- Board of Directors
 - Financial services organizations are required to have the Board of Directors sign-off on all policies per the Gramm-Leach-Bliley Act of 1999.
- Executive Management
 - Executive Management must know that controls are in place to ensure the integrity of accounting information to meet Sarbanes-Oxley requirements.
- Working Groups
 - Working groups should always approve drafts before they are sent to Sr. Management and/or the Board for approval.

Policy Lifecycle



- What is Security Awareness?
 - **A means to enact a change in business culture**
 - An **on-going** program that explains to employees the threats to the information they create, utilize, and disseminate every day, and ways in which they can reduce those threats.
 - Explains their responsibilities in preventing unauthorized
 - **Access**
 - **Modification**
 - **Disclosure**of information assets

- Security has never been a technology problem – It has always been a “people problem.”
- People cause the vulnerabilities but...
- People will always be your first line of defense in ensuring that vulnerabilities do not turn into security breaches.

- People want to do the right thing but they
 - may not know what constitutes the “right thing.”
 - may be doing the wrong thing for all of the right reasons.
 - want to be able to understand and identify the risks.
 - want to be empowered.
 - want to be successful in their job.

- Federal laws require it
- Regulatory bodies demand it
- Customers expect it
- Your company's reputation will depend upon it!

Customers expect that your company will

- **be a good custodian of their information assets.**
- **respect their privacy options.**
- **use information only for the purposes for which it was gathered.**
- **safeguard personal information appropriately.**

- Failure to meet those expectations comes down to one word

REPUTATION

REPUTATION

REPUTATION

- **Will Sr. Management support attendance being mandatory?**
- **Will they announce it as such?**
- **Funding**
 - Deluxe, Shoestring, or no budget at all
- **Lack of Support?**
 - Reminders
 - Gramm-Leach Bliley
 - HIPAA
 - Sarbanes-Oxley

- **Do you have Security**
 - Policies
 - Standards
 - Guidelines
 - Procedures
- **Are they updated?**
- **Does everyone have access to them?**
- **What alternate methods do you have for delivery of them?**
- **Did everyone sign an acknowledgement sheet?**
- **Has anyone read them?**

IGNORANCE IS NO LONGER A DEFENSE

- **To Whom Will You Present The Program?**
 - New Hires
 - Seasoned Employees
 - Long-term contractors/consultants
- **How Will You Present The Program?**
 - In-Person **Interactive** Seminars
 - Interactive Custom CBT
 - Off-The-Shelf CBT
 - Custom Video
 - Off-The-Shelf Video
 - Combination of all or some of the above
- **How Will You Accommodate Special Needs?**
 - Executive Schedules
 - Telecommuters
 - ADA Compliance

- **How Will You Measure Success?**
 - Reduction In Specific Types of Violations?
 - Increased Phone Calls?
 - Reduction In Phone Calls?
 - Increased Funding From Sr. Management?

- **What Is The Theme For Your Campaign?**
 - Do Your Homework
 - What Are The Issues?
 - Where Are They Most Prevalent?

- **Selling Awareness - How Will You Market Your Campaign?**
 - Teasers Leading Up To The Launch
 - Posters Where People Gather
 - Table Top Tents
 - Intranet
 - Internal Mailings
 - Company Newsletter
 - PBX Voice Systems
 - Announcements While on Hold
 - How Do I Get That Trinket?

- **Why Security Is Critical To The Success of Your Company**
- **How Security Ties In To Your Company's Brand Promise**
- **Why Security Is Critical To The Success of Each Person's Job**
- **Who Has Accountability For Security?**
 - **Security Is Everyone's Job**
- **What Are The Problems – Where Are The Problems?**
- **What Can You Do About Them?**

- Common Items Include:
 - **Risks To Confidential Information**
 - Do You Know What Is Confidential In Your Department?
 - Just Listen To That Conversation!
 - Do You Know What Should Be Shredded?
 - Photocopiers and Fax Machines
 - Cell Phones and Cordless Phones
 - Email Content
 - Malware, Spyware & Things That Go Bump In The Night
 - Your Workstation
 - Social Engineering



- Legislation
 - Copyright
 - Examples of Items Covered
 - Business Software Alliance Radio Commercials
 - Gramm-Leach Bliley
 - HIPAA
 - Sarbanes-Oxley
 - California SB1386 and your state's legislative requirements

**Privacy
Notice**



Security “Best Practices”

- Logon-IDs and passwords
 - Do Not Give Out - Even to Management
 - Create an interactive scenario showing what can go wrong when passwords are shared
 - Take the same scenario and provide security options that ensure that the same positive outcome is achieved
- Passwords
 - A way of proving that you are who you say you are
 - Constructing a strong password
 - Password is only secret until you write it down or share it
 - How can you remember all your passwords?

- Email
 - An electronic postcard that is sent in the clear
 - Touched in multiple locations and logged en route to its intended destination
 - Describe how email works so users understand it is not a non-stop trip from one laptop to another
 - Where are the risks?
 - Content, content, content
 - What can you do? – Encrypt
 - What is the ultimate destination of an email?
 - Infinity
 - Privacy is a myth





- Internet
 - Appropriate Use
 - Inappropriate Use
 - Sites That Are Blocked
 - Why Are They Blocked?
 - Can They Be Unblocked For Legitimate Use?
 - » How To Request That A Site Be Unblocked
 - Security Violations Logged

- Malicious Code

**I'VE GOT A VIRUS!
WHAT DO I DO NOW?**

Social Engineering

A method that involves deceiving a user with whatever means necessary to gain information.

- Authority
 - Empathy
 - Reciprocation
 - Consistency
 - Social Validation
 - Phishing
- Ask your audience how often they speak to the CEO of your company. Ask if they would know his/her voice over the telephone.
 - Ask what they would do if someone telephoned them stating that they were the CEO and needed information on a customer immediately.
 - Give them some ideas of how they can spot social engineering in action and questions they can ask to ensure the person on the phone is who they state they are.

SNOOPING

Your 'authorized use' is just that – YOURS!

- Explain that employees have been given access to systems and information to perform their job duties
- Does not mean that they should share that information with others
- Remind everyone to lock their workstation whenever they leave



Physical Security

- **Discuss access to buildings**
 - Card keys and badges
 - Piggybacking
 - Lending your card
 - Handling lost cards
 - Visitor authorization
 - Identification requirements to receive temporary or visitor card
 - Report the loss of your access card to Physical Security immediately.
- **Challenge unknown personnel in your area. DON'T be intimidated. Find out who they are and why they are there.**

- **You have the first 3 minutes to get their interest**
 - Use it wisely or lose them completely
- **Enthusiasm Is Contagious**
 - High Energy
 - Show Passion For The Topic
 - Help Them Feel Empowered



Give me a

S E C U R I T Y

- **Know The Makeup Of Your Audience**
 - Executives
 - Technical Personnel **Address Each Appropriately**
 - Administrative Staff **At Their Level of Understanding**
 - Support Personnel
- **3 Types of Audience Members Always Present - Each have been told by their Manager that they must attend. One type will tell you they**
 - might just learn something
 - are grateful because they did not want to handle what was on their desk
 - want you know they know that security is a barrier and this is a waste of their time.

Be Prepared to Handle Each

- **What Are The Known Security Issues Within Your Audience?**
 - Speak with the Department Head
 - Speak to the Help Desk
 - Speak to Audit

- **Know Your Business Culture**
 - What works at one company may not work in another
 - What works in one department may not work in another
 - Beware of the “cutesy” approach

- Provide examples that they can relate to first on a personal basis and then on a professional one.
 - **What's In It For Me?**
 - How annoying is it when you have your credit card ready, phone in hand, and are ready to place a catalog order only to hear "I'm sorry, but our systems are down. Could you call back in 2 hours?"
 - That vendor just lost your business and you went to a competitor because their system was down. Imagine if that were to happen here at our firm. Customers would be upset, potential customers could be lost, and no one can put a price tag on the loss of reputation.
 - Keeping our systems available is critical, and here is how you can help....

- Make The Session Interactive
 - Start by asking your audience an easy question - one that is impossible from them to get wrong (e.g. What is your company's brand promise?)

Reward Immediately with a trinket
- Create Real Life Scenarios Where Selected Audience Members Apply Knowledge Learned

Reward Immediately with a trinket

- **Use Appropriate Humor to Make A Point**
 - Use real life stories that you have experienced to make a point. Ensure that the stories chosen are relevant to the topic and to your industry.
- **Use Stories of Things That Went Wrong That Became Front Page News**
 - Make the story relevant to your company's business.
 - Make the story memorable – They may miss the technology piece, but they will remember the story. Through the story, they will remember the point.

- **Reward Any And All Participation**

- Get a selection of trinkets that employees will keep in the office and not take home to the kids
- Place slogans on the trinkets such as
 - Stress Balls “Security Is In Your Hands”
 - PC Stress Relievers “Logout Before You Lockup”
 - Key Chains “You Are The Key to Security”
 - Lanyards – “Security Is Everyone’s Job”
 - 5 Click Message Pens – Five security messages – one for each click of the pen.
 - Fortune cookies containing security awareness messages
- No one goes home empty handed – everyone gets a trinket
- There will always be a fidget in the group who needs a toy to settle down and concentrate. Go for the stress balls!

- **When Does Awareness End?**
 - NEVER
- **Keep Security Awareness Fresh**
 - Remind them through new posters of what they have learned
 - Keep them asking questions
 - Keep rewarding good security habits
 - Encourage employees to nominate a colleague who has contributed to the security of the enterprise
 - Present a plaque or other recognition

- Get Ready To Start Again
 - Your theme may change
 - Your material may be updated
 - Your message remains the same
 - but
 - You have new stories to tell
 - and
 - Your enthusiasm is even more contagious



Anne E. Terwilliger, CISSP
President



Accentuate **SECURITY**

P.O. Box 24002

Cleveland, OH 44124

Phone: (440) 995-5555

Fax: (440) 995-5085

Email: aeterwilliger@accentuatesecurity.com

www.accentuatesecurity.com