CONF-9005106--2

SAND--90-0373C

DE90 008499

# DEVELOPING A COMPUTER SECURITY TRAINING PROGRAM

We all know that training can empower the computer protection program. However, pushing computer security information outside the computer security organization into the rest of the company is often labeled as an easy project or a dungeon full of dragons.

Used in part or whole, the strategy offered in this paper may help the developer of a computer security training program ward off dragons and create products and services. The strategy includes GOALS (what the result of training will be), POINTERS (tips to ensure survival), and STEPS (products and services as a means to accomplish the goals).

**GOALS.** All personnel through awareness and training must (1) be aware of the scope and magnitude of risks and threats to computing resources and the consequences of problems resulting from them; (2) accept, learn, and perform their computer security responsibilities; (3) be able to identify actual and potential threats and vulnerabilities to resources; (4) prevent waste, fraud, abuse, and misuse of computing resources.

**POINTERS.** (1) All forms of information may be considered designed messages. Messages are designed for different groups through the training program. (2) A training program contributes to company compliance but is not solely responsible for it. (3) Awareness and training is a process; developers must pace themselves and the company. (4) Like other projects, while finishing one product, the developer will be continuing another, and starting yet another. It requires constant attention, energy, and deadlines (flexible deadlines). (5) Computer security trainees are also customers, advisers, and critics who have good ideas. They often say what would be the most useful. (6) Products should be designed and formatted for easy and convenient updates and should also include dates and distributions. (7) Computer security information does not solely belong to the computer security organization nor just one person with expertise. Information must be passed on to others who need to know. (8) Credibility and good public relations should be part of the messages. Personnel will

**DISCLAIMER**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

## DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

## DISCLAIMER

**Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.**

generally comply with requirements; they just need to know what the requirements are. Nonetheless, even after reiterating messages countless times, there will be a few who say "nobody told me," and some who make a sport out of challenging computer security. (9) Adequate support and resources must be soundly in place before an official announcement is made of the training program. (10) People must have current information that works in their "real world. " Information must use clear and consistent terminology, provide names and numbers for further information, incorporate others' ideas and suggestions, and be honed to the computer security duties.

**STEPS--support products and services.** Training personnel should collect material from within the company, outside sources, and develop products and services for the training program.

**1. POLICY.** Pre-existing written material (policy statements, procedures) must be located and gathered; and, support services (cooperative people and key contacts in mail rooms, copying services, and keepers of distribution lists) should be identified. Policy statements and procedures, noting topics, dates, sources, and distributions should be reviewed and organized. Quick analysis will provide a picture of who knows what about computer security and when they learned it. If dates, topics, and distributions are old and out of sequence, it is likely that personnel are confused about their responsibilities. Unfortunately, the exception may be the few who still follow procedures written in an obscure memo in 1962 by someone nobody remembers.

Written material may include policy statements and procedures in the form of memoranda, handbooks, instructions, forms, letters of appointment, or documents to or from DOE, the company, or others. Usable material may be arranged into manuals for a policy baseline.

**2. STANDARDS AND PROCEDURES DOCUMENTATION** should be created, either separate ones for PCs and multi-user systems or an all-in-one document, for users of classified and unclassified data. The document (manual, handbook, etc.) differs from policy because it is more comprehensive, broader in scope, and is interpreted for application in the company. Users need the "what's" and "how to's" to fulfill their responsibilities. Procedures also serve as a reference guide, textbook for training, and criteria for internal reviews. Users are employees and contractors who manage, design, develop, operate, or maintain computing resources, and share most basic responsibilities. Documents designed in sections and in a loose-leaf format are easiest to maintain. A list of acronyms, a table of contents, and an index will add to the document's usability. Since the document is for general end users, it should include the topics listed under General end user below. Topics may overlap between groups of personnel,and the depth and detail of information may differ.

**3. GROUPS AND TOPICS.** The following are groups with similar computer security responsibilities and lists of suggested topics for these particular groups.

**New hires:** Computing resources, the company's protection policy, the concept of special protection requirements for classified and sensitive unclassified, and the requirement to determine sensitivity levels before accessing or processing data.

**Renewed Q clearance:** Reminders of topics for new hires, references to contacts and resources in the computer security organization

**General end user:** Protection against waste, fraud, abuse, and misuse, with examples; general threats--risk assessment; determining sensitivity levels before accessing or processing data; definitions of sensitivity levels; security plan requirements; computer media handling, storing, marking, labeling, sanitizing, disposal; sharing resources; document accountability; password protection; incident reporting; virus protection; audits

**(Secretaries:** Secretaries are end users also, but they need special emphasis on PC security and document accountability since they are asked to handle others' work.)

**Host system user:** Special requirements that apply to host systems and their users (e.g., need-to-know; vault guidelines; maintaining current access lists; visitor and escort procedures; login-logoff instructions; checking login screen for record of access; password guidelines; notification of changes; or other system-specific security guidelines)

New and continuing CSSO or ACSO: Duties and responsibilities, reference material, and guidelines for writing and maintaining security plans

System administrator: Password systems, computer media, audit trails, random file monitoring, procedures to use when making system changes, physical security, elements of security plans and backups, disaster recovery

Operations: Physical security, computer media, visitor and escort procedures, hardware and software guidelines, contingency planning, emergency systems, disaster recovery

Supervisors: Security plan requirements, threats, incident reporting, infractions, audits, signature authorizations that involve computer security (password requests and security plans that permit access to controlled information, clearance requirements, proper use of computing resources)

Upper management: Risk assessment, contingency planning, threats to resources, changing technology, legal implications, overall consequences of computer security problems and issues

**4. USE A VARIETY OF PRODUCTS AND SERVICES TO SUPPORT TRAINING THROUGH TEACHING, ADVERTISING, AND PROMOTIONS.** It is not enough to say, "You must learn computer security rules." Personnel need to know exactly what is meant, and want to know why they should bother.

Effective messages must be sent via a number of avenues. Messages seen or heard repeatedly from different angles reach their targets. For example, a password rule that is covered in a reference document, a newsletter article with an illustration, a poster, and during a live presentation has a good chance of becoming office routine.

Delivery avenues must be planned. If the training program is short on manpower or budget, it is better to spend a little time producing two simple items that have longevity than to create one slick item that will be obsolete in a year. It is better to spend the first six months buying some posters and writing a reference manual or procedures than devote six months to creating one grand poster. As the training program emerges from developmental stages, more time and energy may be devoted to polishing one item.

Advertise everything: the training project, rules, products, services, and computer security itself.

**Logos** Logos identify computer security. The company will learn to recognize computer security as an official entity. Logos will be around for a while, so they should be simple, appropriate, and acceptable to the majority of personnel in the company (e.g., a funny cartoon character may be too juvenile and pictures of chains, locks, and spies may be too negative).

**Posters.** Brief, repetitive messages seen out the corners of our eyes often become engraved in our memories. They may influence our attitudes and behaviors. Posters may be purchased if time or resources prohibit creating them. General Motors and Vanguard Marketing Services offer several designs that are conveniently sized (8 1/2" by 11"). Interesting shadows and highlights, brilliant colors, unusual settings, and asymmetrical layouts will attract attention of personnel who see monotone black and white, even margins, and file cabinets daily.

**Bulletin boards.** Ask others to watch newspapers and magazines for articles about computer security. Bulletin boards work best located near snack bars, restrooms, and stairways. News articles reinforce the reasons for computer security policies through "real world" scenarios. Hard copy of vugraphs and novelties are also good to display.

**Newsletter articles, company bulletins.** Newsletters or company bulletins are avenues for announcing special colloquiums, policy changes, or products and services available. Someone else must deal with final copy preparation, distribution lists, and reproducing copies. However, others may impose deadlines, formats, and approval cycles on the articles. Also, newsletters are often written for special groups, so messages may not reach all personnel in need of the information.

**Templates, outlines.** Models for security plans are a great help.

**Forms.** Though forms are not strictly training material, they can be designed to instruct. Information may be added to forms used for reporting incidents, requesting and accepting passwords, controlling modem usage, inquiring about sensitivity levels to be used on equipment being ordered, and tracking the life and death of secure computers and media.

**Novelty items:** Logos and short slogans on novelties promote awareness. Items that have high visibility and continual use are most desirable. Examples of inexpensive paper novelties created in-house are mock-ups of computer media or colored index cards with basic procedures printed on them.

**Checklists and lists:** One of the most useful items for CSSOs and end users is a simple checklist. A quick list for checking duties or points of system security is efficient and concise. Also, it is good to periodically distribute a list, by division, of accredited PCs. PCs are difficult to keep track of in large companies.

**Presentations and vugraphs.** Live presentations will get the company on the computer security band wagon. A variety of material must be created on required topics for each group (e.g., end users, CSSOs). Speakers may be available in the organization, company, or from the computer security community outside the company.

While personal end-user training is very important, it is impossible for one person to personally train everyone in a large company. A good start is for a computer security representative to voluntarily speak at user group or division meetings. There will be numerous invitations when the word gets out.

Trainers learn first hand about computer security too: the company's misconceptions, anxieties, anger, strengths, and weaknesses in computer security. During the process, trainers will discover ways to customize talks, make and reuse vugraphs, cope with stage fright, establish relationships for the computer security organization, promote materials, and set the stage for later training requirements.

Material developed for live presentations (e.g., vugraph transparencies and hard copy; handouts, etc.) may be organized for reuse by topic or in sets for different groups. For easier control, vugraphs may be numbered and filed in a binder. Hard copies may be made of the vugraphs and set up in file folders with corresponding numbers. Requested material may be pulled conveniently from the file folders.

A file of electronic and cut-and-paste art is useful too. For example, a picture of bugs crawling on a computer says "computer virus" in an interesting way.

**Creating a computer security bulletin.** An internally created bulletin is one of the best training tools. Distribution may be to all employees or may be more limited. It should be one page, front and back, with news articles written in inverted pyramid style.

**Memoranda.** Memoranda are *official* avenues for communicating with supervisors, upper management, system administrators, and CSSOs/ACSOs about policies and requirements. Current distribution lists are essential.

**Booklets and pamphlets.** Descriptions of computing resources and the company's policy on protection in brief booklets are adequate for new hires who get overwhelmed with information. For other personnel, information may be added to company handbooks: code of conduct, termination of employment, ordering computer software and hardware. Information may also be added to computer manuals.

**Videotapes.** Videotapes are wonderful resources. Sources (i.e., AT&T, Commonwealth, DOE, etc.) are advertised in most computer security literature. Cost and time constraints prohibit most companies from making their own.

**5. Tracking and logging training.** Large companies should have a database and matching log sheet to track training, print lists and labels (CSSOs, accredited PCs, etc.), and to use in creating reports. Here are some suggestions for the database and corresponding log sheets: (1) **Date and applicable division numbers or CSSO** names. (2) **Type of training** (seminar or class, material circulated, meeting, company-wide presentation or distribution, briefing 1-5 persons, outside conference). (3) **Training module** (module = specific topics for each group; see number 3 in this paper, Groups and topics). Suggested modules are General Awareness, General User Basics, Shared System Basics, Administrative Planning and Management, Contingency, System Security, Other). (4) **Resources used** (video or film, speaker, publication, memo, all). (5) **Sponsor** (computer security organization, CSSO etc.)

**6. Putting the training program in place.** One person may be assigned to plan and develop a training program, create and maintain products and resources, and generally ensure its ongoing status, but options must be created to assist with implementation.

Training based on the modules using the products and services must be required. The CSSM may sign a memo stating the requirement that supervisors must ensure general user basics for personnel at the division level and CSSOs must ensure training for system users. Training for all end-users could be accomplished by doing so. The training program would provide support and resources.

Training for CSSOs, system administrators, and management should be provided by the computer security organization.

**Summary.** There are no dragons in dungeons to fight, or quick and easy ways to develop, implement , and maintain a training program. Training is a full-time job that requires constant and dedicated effort.