**Security Awareness – are your users "clued in" or "clueless"?**

Robert Held

May 23, 2001

## Introduction

A sound security policy is the foundation of any successful security program. The policy defines the organization's overall posture toward security – whether it is very restrictive, allowing little or no leeway in access to data; or if is it more permissive, giving users more latitude in their actions. In either case, the policy must be the first step toward achieving an acceptable level of security.

But to what avail is even the best policy if those who are affected by it do not know of its existence or understand its contents? None! This is why security awareness (making users aware of what is expected of them in protecting the organization's data) is an equally critical element in a successful security program. Without this awareness, users cannot be held responsible for failure to comply with policy; and may adversely affect the confidentiality, integrity and availability of your organization's information.

Users must not only know about the policy's existence, they must understand the contents of the policy, they must be aware of their responsibility in achieving the security objectives of the organization, and they must be aware of the consequences for non-compliance. This user education can be accomplished most effectively through a well-designed security awareness program.

## Where to begin?

Prior to developing a formal security awareness program, you will need to obtain the approval of senior level management to expend budget monies on this effort. This is often the most difficult step in establishing a security awareness program. Security is all too often viewed as an obstacle to achieving the objectives of the business. You must convince senior management that security awareness is a worthwhile – even vital – element in protecting the information assets of your organization.

In order to obtain senior management approval, you will need to provide them with an explanation of the benefits of a security awareness program. Unfortunately, these benefits are often difficult to quantify. Fortunately, however, the FBI and Computer Security Institute (CSI) have done some of this work for us! According to the CSI, "The findings of the '2001 Computer Crime and Security Survey' confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting." The following highlights are taken from this CSI/FBI survey:

- Eighty-five percent of respondents…detected computer security breaches within the last twelve months.

- 186 respondents reported $377,828,700 in financial losses.

- The most serious financial losses occurred through theft of proprietary information (34 respondents reported $151,230,100).

- Ninety-one percent detected employee abuse of Internet access privileges.

These numbers can be used to help persuade organization executives of the need for a security awareness campaign. As stated by Patrice Rapalus, CSI Director, "Each year, the influence and impact of the CSI/FBI Computer Crime and Security Survey grows. It is an invaluable tool for information security practitioners….to get the attention of their CEOs, CIOs and CFOs…..".

While obtaining approval for a security awareness program may be a difficult task, it is essential to the success of your entire security program. Without the approval and support from your senior management team, your security program will lack credibility and will be destined to fail.

**The next step**

After obtaining the "go ahead" to develop a security awareness program, the next step is to define the overall scope and objectives. This involves answering the following questions:

- Who is my intended audience? You may target different groups of employees using different methods. It is important that you recognize the different needs of each group of users in order to develop the most effective approach.

- What is my intended message? Are you covering the corporate policy, an industry standard, or communicating recent security events in the news? Each of these topics can provide an increased awareness of various aspects of information security; but each may also require a different approach in getting the message across to your intended audience.

- What result am I trying to achieve? In some cases you may simply be trying to provide new information to your users, in others you may be trying to change or invoke a specific pattern of behavior. This intended outcome may dictate a different approach to your presentation.

- What communication method am I going to use? The approach you take in presenting your message to your users will vary based upon the answers to the previous questions. Consider what communication options you have available to you and which will have the greatest chance of achieving your objectives.

As you continue to define/refine your security awareness program, additional detail will begin to develop in your plan. It has been my experience that brainstorming sessions are

particularly useful during this phase of development. Through these sessions you will quite likely come up with new approaches that hadn't occurred to you before. Be creative – this is the best way to capture and retain the attention of your audience. As your plan develops, you may end up with something along the lines of the following outline:

- Intended audience – although there can be multiple divisions of employees within each organization, listed below are three primary groups of employees and some things to consider when developing your security awareness presentation.

    - Executive-level employees – Due to busy schedules and heavy demands on their time, it is imperative that any security awareness program directed toward this group of employees must be brief! Be over-prepared – you will probably receive questions! A failed effort in bringing your message to this level of users will have a severely adverse impact on the credibility of your security awareness program and may bring about its demise.

    - Management-level employees – This level of employee will take their cue from the executive level employees. If the organization's executives support the security awareness program, the management team will at least listen to your message. They are responsible for the compliance of their subordinates (so they will need to understand your message); but they are also focused on the continuation of business and the bottom line. Again, efficiency in conveying your message is of very high importance.

    - Staff-level employees – This group of users is the "hands on" group with the most potential to impact the security of your information environment. These are the users that have daily access to customer data, business data, and outside contacts. Their actions, whether intentional or accidental, can impact the confidentiality, integrity and availability of your data! You will need to provide the most detail to this group – but, as with every level, in a time-effective manner.

- Intended message – There is a wide variety of topics you may choose to address through your security awareness program. Listed below are three primary categories.

    - Policy – Obviously you need to make your users aware of the existence of the policy; but you also need to inform them of the content of the policy and how this applies to them. Simply stating that the employee must do "such and such" in order to comply with policy will not be effective. You need to inform the user why this makes a difference to them!

    - Procedures – Understanding the policy is all well and good – but you also need to inform your users of specific procedures to follow in order to comply with the policy statement. As an example, you may have a policy

statement that says, "Users must select secure, hard-to-guess passwords." By informing the users of how to select a good password (such as selecting a password that is at least six characters long; avoiding dictionary words; using letters, numbers and special characters; etc.), you will greatly increase the chance that users will comply with the policy.

- Recent Events – As the song says, "Ain't nothing like the real thing!" This is certainly true in security awareness. Informing users of recent hacks or employee terminations for policy violations brings the message home. This is especially true the closer to your organization the event was. Ideally, if you can communicate internal investigations and their outcome (being careful not to disclose any confidential information), you will prove that it can happen to anyone, anywhere.

- Method of communication – There is a very wide range of communication methods that you may use to present your message. It is a good idea to use multiple forms of communication in order to ensure that your message reaches the broadest number of users possible. Several examples are listed here.

  - Company Intranet – Most organizations have an Intranet for posting internal information. This is an excellent place to post the security policy, as well as a number of security awareness features. One thing to keep in mind is that to be effective, the content will need to be changed regularly.

  - Newsletters – Nearly every organization has at least one form of company newsletter (and may have several). This is a convenient and cost-effective way to get your message out to a broad number of users. However, it is important that you do not over-utilize this means of communication as the audience may become conditioned to your message. It is also quite common that fewer users read the newsletter on a regular basis than may notice other forms of communication.

  - Posters – Posters can be a good way to communicate your message. In order to be effective, they must catch the viewer's attention. This can be achieved through use of bright colors, humorous characters, catchy slogans, and so on. It is also recommended to make them larger than standard letter size so they stand out, and change or rotate them regularly to keep the message fresh and inviting. Avoid cluttering the poster with too much information – stick to one primary issue. Placing your posters in high traffic areas (in the coffee room or cafeteria, near restrooms, by conference areas, etc.) will increase exposure.

  - Puzzles and contests – Hands-on learning is often the most effective because the student gets to participate, which reinforces the message. There are a number of activities that can be utilized in this regard. A few examples of them are:

- Cross-word puzzles
- Word searches
- "Spot the violations" cartoon
- Word scrambles

- "All-hands" meetings – Often, other departments (such as Human Resources or the Legal Department) will conduct meetings for all employees to cover such topics as sexual harassment, drug abuse awareness, workplace conduct, etc. This is an excellent opportunity for you to collaborate with these other departments to incorporate your information security message into part of their presentation.

- Broadcast email messages – This is an especially effective way to communicate messages on the proper (as well as improper) uses of email itself!

- Hardcopy memos sent through inter-office mail – One topic you may choose to use "snail mail" for is proper handling of printed documents. Too often we concentrate on computer-stored information and forget that a great deal of sensitive material is still disseminated in printed form. Our security awareness program should include all forms of company information!

- Security memos printed on paycheck stubs – Every employee gets a paycheck and we are usually interested in it! This is a great opportunity to extend a brief security reminder to all employees.

- Videos – Videos can be one of the most effective, but also among the most expensive, forms of communication. If you have an adequately large budget for your security awareness program, or if you will be able to reuse the video over and over again (such as for new-employee orientation), then a security-related video would be an outstanding tool in your security awareness program. But, be prepared to spend big bucks, as an average cost of producing a video is $3,000 per finished minute. Several companies also offer professionally produced videos for sale.

**Putting the plan into action**

After determining the audience, message and approach, it's time to "roll out" your security awareness program and put your plan into action. Regardless of the communication method you have selected, there are some standard guidelines to keep in mind to make the process most effective.

- First, explain why security is important. People are more likely to comply with your policies and procedures if they understand their importance to the organization, department and individual; and if they understand how better security practices may help them achieve the objectives of their own position.

- Keep the training sessions as brief as possible. It is normally recommended to keep these sessions to no more than one hour. For print media, keep your message to less than one page (1/2 a page is even better). If the length of the program (or article) is longer than the recipient's attention span, then much of the message will be lost.

- Provide the audience with some form of reminder of the objectives of the program. A small trinket such as a key chain, mouse pad, coffee mug, paperweight, etc. will help remind them of the security topic. Every time they use that object, they will be reminded of your message. This will provide an on-going reinforcement of the importance of information security.

- Don't overdo it! Although you know there are a vast number of topics you want to – perhaps even need to – inform your users about, avoid the temptation of covering too much information at one time. If you do, again, much of your message will be lost.

- Awareness requires continuous efforts to keep the message fresh and in front of everyone. Security awareness is most effective when it is presented on a regular basis. I have found that a good rule of thumb is to try to make some form of security contact with every group of users on the average of once a month. This keeps the security message in front of users without burdening them with too much information at once.

**Where do we go from here?**

We all know that information security is critical to the welfare of the organization; and that security awareness is vital to the success of the information security program – but if we never put that knowledge into practice, we are destined for failure. We know what the problem is – our users are not adequately prepared to meet the security challenges they face day after day; and we know the solution – that only by developing and implementing an effective security awareness program will we raise the awareness of our employees to a level that will provide an acceptable response to the security challenges they face. But we've known these things for years! In an article on "The Information Security Program Maturity Grid" in Information Systems Security, Summer of 1996 (the timeframe when I first became involved in the Data Security group at our organization), there are multiple references to the need for an effective security awareness program in order to advance along the maturity continuum for a security program; and yet five years later we are still addressing the same issues – many of us are continuing to struggle with the task of obtaining approval from an executive management group that still views

security as overhead, some of us have obtained this approval and are in the process of defining how our security awareness program should look and feel, fewer of us have launched a structured security awareness program with any regularity, and even fewer have achieved the level of maturity in a security awareness program that achieves the objective of making our users aware of their role in promoting and practicing proper information security habits.

**Conclusion**

Security awareness has never been more important. As security threats become more complicated and we become more inter-connected, it is imperative that we not only develop, but fully implement quality security awareness programs for the benefit of our users and organizations. By achieving this objective, we will have users that are "clued in" to the importance of information security and how it affects the organization, department and individual. Without this awareness, our users are "clueless" and an incident waiting to happen!

**Citations**


Rudolph, K, CISSP, Computer Security Handbook, 4th Edition, Chapter 29.
URL: http://nativeintelligence.com/awareness/CSH CH29 KR.PDF (18 May 2001)

Mitretek Systems. "Security Awareness."
URL: http://www.mitretek.org/mission/securityprivacy/securityawareness.html (18 May 2001)

Computer Security Institute. "Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar."
URL: http://www.gocsi.com/prelea_000321.htm (18 May 2001)

Native Intelligence Article 2. "Getting the Word Out."
URL: http://nativeintelligence.com/tmart.asp (18 May 2001)

Peltier, Tom, CISSP. "How to Build a Comprehensive Security Awareness Program." Computer Security Institute Computer Security Journal, Volume XVI, Number 2. 23-32.

Stacey, Timothy R., "The Information Security Program Maturity Grid." Information Systems Security. Auerbach Publications. Summer 1996. Vol. 5, No. 2. 22-33.