Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Secure This: Organizational Buy-in (A communications approach)

In order for a security plan to be effective, it must enjoy full support from an organization's executive leadership. Seems like a simple truth? It is, but securing that backing is not as simple. One of the roles the information security officer must fill is that of a salesman, not only to corporate leadership but also to rank and file staff. Top-to-bottom organizational buy-in is one of the most important elements that will dictate whether an information security plan, and its associated policies and procedures, are e...

Copyright SANS Institute

Author Retains Full Rights

AD

Wendy E. Ady
Assignment Version 1.2e

Secure This: Organizational Buy-in

A communications approach

In order for a security plan to be effective, it must enjoy full support from an organization's executive leadership. Seems like a simple truth? It is, but securing that backing is not as simple. One of the roles the information security officer must fill is that of a salesman, not only to corporate leadership but also to rank and file staff. Top-to-bottom organizational buy-in is one of the most important elements that will dictate whether an information security plan, and its associated policies and procedures, are effective. This paper will discuss the importance of buy-in and will recommend methods for soliciting and securing buy-in using a communications theory perspective. It is not the intention of the author to explore the topic in depth; rather, the purpose is simply to offer ideas which merit further exploration and discussion.

Importance of buy-in at all levels

Indeed, it is the human element that poses one of the highest risks to information security. Operating systems can be hardened, virus scans can be conducted on a regular basis, and hardware can be physically secured; however, if employees of an organization do not understand and embrace basic information security best practices, much is for naught.

Executive Leadership: The need for executive level sponsorship is two-fold. First, to assure staff buy-in, corporate leadership needs to visibly and consistently validate the security policy and procedures. If the executive level doesn't fully support the security program, there will be little reason for the rest of the organization to do so (NIST, 2001). Second, it is necessary to ensure that funding will be in place to support the program. A comprehensive information security system requires a significant initial investment of human resources, hardware, and software. In addition, because the technology environment and the types of security risks are always changing, there is an ongoing need for upgraded security tools and staff training.

IT Department: Unwavering support for the corporate security policy and procedures is especially important within the information technology department. Often it is difficult to reach a consensus regarding the best approach to protect corporate IT resources. In the IT field, there are many, many ways to reach a similar end. Although helpful in some ways, the many combinations of variables can also be a hindrance. While it is important to note that differing opinions and the free expression of conflicting ideas are valuable in the development of the comprehensive security plan, it is equally important that, once a plan has been constructed, everyone in the IT unit present a unified front. Nothing

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

undermines a security policy more than IT professionals debating the merits of the security program or criticizing it in the more public organizational arena. If the IT department can't agree that the policy and procedures are important and worthwhile, soliciting non-technical staff buy-in is extremely difficult, if not impossible.

Employees and Other Users: Organization-wide support is a necessary element for a successful security model. In fact, people throughout the organization represent a critical functional layer in an effective defense strategy (Hasse, 2000). Simply put, locks on the doors and windows are useless if people intentionally or inadvertently open them from the inside. People who do not understand and embrace the corporate information security policy pose a significant risk. "There is a great deal of publicity about intruders on computers systems; yet most surveys of computer security show that, for most organizations, the actual loss from 'insiders' is much greater" (Fraser, 1997).

Once the information security officer has recognized the importance of organizational buy-in, how does he or she go about creating a security-conscious culture throughout the organization? The obvious answer is to establish an awareness and training program, but the next, and more difficult step, is to determine how best to deliver the message within such a program.

Developing organizational buy-in through a security awareness program

Security awareness can serve several functions and can be enabled through a variety of methods. It is the goal of awareness to move people to care about security (NIST, 1996). Through increased awareness people learn the ramifications to the organization, its mission and its goals, when security practices aren't followed. Awareness efforts differ from training in that the latter is more formalized and structured; training will be discussed in a later section.

Often used methods for increasing security awareness can range from special events, posters, email, and occasional reminders of the basic security information learned in training (Vallabhaneni, 2000). In the following paragraphs, this paper offers an often overlooked aspect and approach: that of developing community.

Security as part of the community: In communications theory, the term community is defined as of a cohesive group of people having a unifying theme and being held together by different things that they share, such as work, territory, ideals and skills (Wilmont, 1995). Security professionals need to demystify themselves and their profession so as to become a part of the organizational community, and concurrently help people understand their own responsibilities within that same community. This will go a long way towards the inclusion of information security consciousness in the corporate culture. This is not advocacy for the removal of accountability, but rather a suggestion that a holistic approach to the management of the human elements of a security plan is best.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Community and personal responsibility: Communications theory recognizes that human beings have a natural tendency to want to be part of a community and work toward a common goal. This involves both a shared understanding of the importance of community norms, and the responsibility each person in the community has in maintaining those norms. Adapting communications tools and techniques to an information security awareness program should work toward that end by emphasizing effective communication to targeted audiences, and should be multi-faceted, as the organizational community is.

Community norms instead of brute force: Looking at a real-world example in the law enforcement arena is helpful in understanding the shift from a brute force to community development concept, especially because of similar protection goals of law enforcement and information security. Over the course of many years, a rift had developed between inner city communities and members of the local police forces. As a result, police departments needed to alter their approach to policing neighborhoods, shifting away from brute force tactics and toward improved public relations through the use of trading cards, walking patrols, and other initiatives that involved personal contact with the community. Police departments learned that they are more effective when they are viewed as a part of the community, and that law abiding people are more willing to cooperate in productive ways when they feel involved and valued. With the help of neighborhood groups, more and more individuals throughout the community now view the police as fellow team members, all working toward the common goal of securing and protecting the inner-city environment.

A business marketing strategy: In designing the program itself, a business marketing strategy called AIDA can provide a good basis from which to work (Johnson, 2000). AIDA stands for:

- Getting the **Attention** of your audience.
- Developing an **Interest** in your message.
- Creating a **Desire** for your message.
- Encouraging the audience to take **Action**.

Attention: Over the past twenty years people have become increasingly familiar with computers. This familiarity can lead to a false sense of security and complacency. This is especially true in the computing environment because the threats are not always visible to the untrained eye. Computer professionals can see the signs of the threats coming across the wires; casual users might only notice that the system is slower than usual, if they notice anything at all. The awareness plan must include material that will garner the attention of users and address any misconceptions they may have.

Interest: It is often recommended that people use widely-known, large scale, high-impact incidents to grab the attention and interest of the audience and help them relate information security to real life situations. This approach can often backfire. Because only a few of these incidents are widely publicized, people get

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

the impression that incidents are infrequent. Furthermore, they can dismiss the example as being too outlandish and high profile, can miss the message that an incident could happen to them and/or to the system they use. The stories and examples should be relevant to the audience and organization.

Desire: Creating a desire among users to follow good security policies and practices is one of the biggest hurdles that the awareness program will face. This is the area in which corporate community and culture works to encourage conformance to acceptable norms. In general, American culture values the basic tenets of information security – confidentiality, availability and integrity – but in an abstract way. We want to know that we can keep certain things private (confidentiality); we want to have the ability to get things we need (availability); and we want the other people we encounter to deal with us fairly (integrity). For those people who are less ideological, the desire to avoid liability can also work. Overall, tapping into individual or community values is an effective approach to creating desire.

Action: People who have been engaged by the attention, interest, and desire components will be more likely to follow procedures and policies that are taught in security training courses. In fact, they may actually attend security training that isn't mandatory. The goal of an information technology security awareness program must be to move people to care about security and take actions that reflect that commitment.

Security awareness programs should be designed to set the stage for training by changing organizational attitudes to realize the importance of security and adverse consequences of its failure, as well as remind users of the procedures to be followed (NIST, 1996).

Developing organizational buy-in through a security training program

In *Generally Accepted Principles and Practices for Security Information Technology Systems*, the authors set out seven primary steps to establish an effective computer security training program. They are:

1. Identifying program scope, goals, and objectives.
2. Identifying training staff.
3. Identifying target audiences.
4. Motivating management and employees.
5. Administering the program.
6. Maintaining the program.
7. Evaluating the program.

Key aspects: There are also key aspects of information security that should be included in the training, and addressed to a level that is appropriate for the audience.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1. Identification of the aspects of the corporation and its business that makes it a target for particular incidents.
2. What is expected from users.
    - Users should be made aware of how the computer systems are expected to be used, and how to protect themselves from unauthorized users (Holbrook, 1991).
    - Users should be told how to properly manage their accounts and workstations (Holbrook, 1991).
    - Users should be told how to detect unauthorized access to their accounts (Holbrook, 1991).
3. Accountability and legal issues.
4. Identify and report security incidents.

Information and knowledge: In developing an information security training program, insight into the nature of learning is important. A particularly applicable statement can be found in Organizational Communication, written by Andrews & Herschel, 1996.

> *Information does not always lead to understanding. In contrast to information, knowledge goes beyond the facts, connecting and explaining them. Knowledge further refines information and seeks to reconcile seemingly disparate findings. It is knowledge, not information that can best contribute to empowerment (p.5).*

As an example of this, one need only look at the large number of hoax e-mail messages that are forwarded through mail systems every day warning users of dangerous viruses. These denial-of-service attacks are intended to overload email servers, and are based on the expectation that well-intentioned individuals will attempt to keep viruses from infecting friends and co-workers by forwarding the hoax message to large numbers of people. These individuals truly believe that they are acting in a security conscious, responsible manner. However, if these people had a basic knowledge of information security, they would be less likely to react to these hoaxes.

A communications specialist can help

Understanding how to communicate to differing audiences is one of the determinate factors in how effective awareness and training efforts will be. Together, awareness and training programs can enable users to embrace and understand basic information security practices. These programs should be structured to speak to the community of users, and one cannot stress enough the notion of know thy audience.

Using communications tools effectively requires a certain degree of expertise which may not already exist within the typical security organization. Since organization-wide support is such an important part of a comprehensive security plan, it is wise to solicit the input of a communications professional through contract or employment. This person can help craft and facilitate communications at all levels. As is shown in the next section,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

communication complexities are the norm and should be taken into consideration to the extent possible.

Complexities in transmitting the message: The message, messenger and audience bring with them experiences, attitudes and beliefs that alter the rhetorical situation - comprised of exigence, audience, and constraints (Cooper, 1989). Maletzke's Model of the Mass Media shows the complexities of communicating from a different perspective:

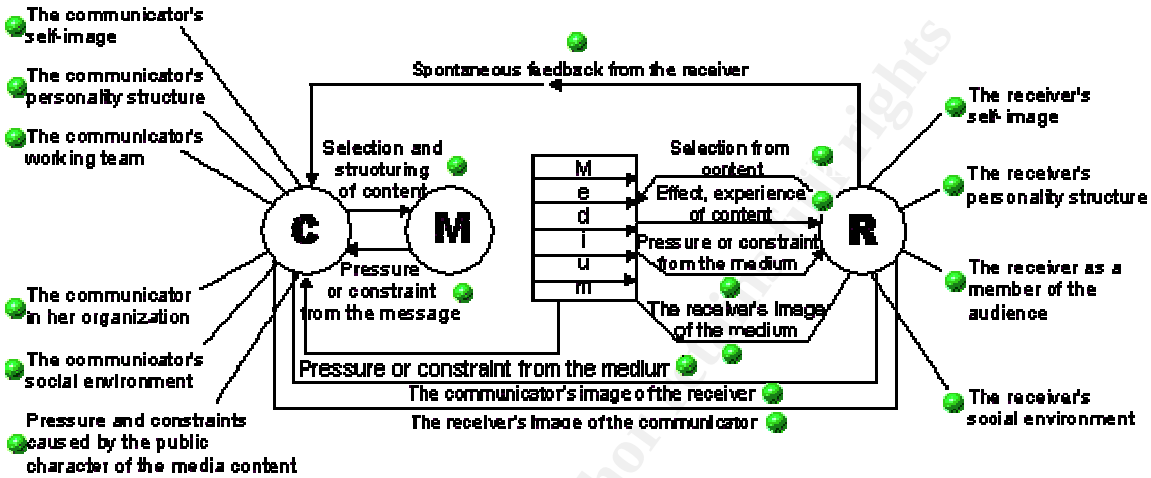

Figure 1. Maletzke's Model of Mass Communication (1963)

While models differ, the issue of complexity remains. This poses an obstacle for the security officer who is often not familiar with the intricacies of communication theory and practice. If communication strategies are not designed with discipline and purpose, people may discount the message.

The value of conflict: In anticipating conflict surrounding security policies and procedures, it is only natural to brace oneself for that conflict. However, communications theory would encourage a security officer to embrace that conflict and use it constructively. This will go far in assuring that the security program becomes relevant and appropriate to the organization. Invariably, people will want a chance to have their opinions on matters heard, and transitioning these opinions into support for the program can be tricky but worthwhile.

Through effective use of communications theory and practice within information security awareness and training programs, organizational buy-in can be secured. For these and related reasons, an individual with savvy in both communications theory and information security would be a valuable asset to a security unit and/or IT division.

Final thoughts

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In a community, members share common norms and values. In addition, they have information that helps them contribute to the community's stability and well-being. A comprehensive information security awareness and training program can be the vehicle for establishing and reinforcing a sense of community within the organization. As the circular process of identification with the corporate community having the effect of begetting more involvement in it, an organization can expect more wide spread buy-in for the culture. If part of the cultural norms and values are supportive of security, one can expect that the security plan will enjoy increased buy-in as well.

As with any endeavor that seeks to alter attitudes and behaviors, consistency is key. Information awareness and training plans are not simply implemented programs. In fact, much on the job training occurs through example. Many communication theorists recognize the importance of the informal network in passing along the culture of the organization. In this case, a security-conscious community is the goal. It is important that everyone who is involved, either through organized presentations or daily example, is delivering the same message.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References:

National Institute of Standards and Technology. "An Introduction to Computer Security, 800-12." June 19, 2001 http://csrc.nist.gov/publications/nistpubs/800-12/

Hasse, Cathrine. "Information Security Awareness." 2000. http://www.sans.org/newlook/projects/cap_welcome.htm

Fraser, B. "Site Security Handbook." RFC 2196. September, 1997. http://www.ietf.org/rfc/rfc2196.txt

Vallabhaneni, S Rao. CISSP Examination Textbooks. Vol.1: Theory. Schaummburg, SRV publications, 2000.

Wilmont, William W. Relational Communication. New York, McGraw Hill, 1995.

Johnson, John. "Presenting Security Awareness Training At Your Company." January 26, 2000. http://www.nwfusion.com/newsletters/sec/0124sec.2html

Swanson, M., Guttman, B. "Generally Accepted Principles and Practices for Securing Information Technology Systems." NIST, September, 1996. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Holbrook, P., Reynolds, J. "Site Security Handbook." RFC 1244, July, 1991. http://www.ietf.org/rfc/rfc1244.txt

Andrews, P., Herschel, R. Organizational Communication; Empowerment in a Technological Society. Geneva, Houghton Mifflin, 1996.

Cooper, Martha. Analyzing Public Discourse. Prospect Heights, Waveland Press, 1989.

Maletzke's Model of Mass Communication (Fig.1) image: www.cultsock.ndirect.co.uk

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Questions

Multiple Choice

1. What does the business marketing acronym AIDA stand for?
   a) Attention, Interest, Desire, Action
   b) All Individuals Deserve Attention
   c) Alternative, Investigation, Decision, Action
   d) Assertiveness, Initiative, Demonstration, Awareness

Answer: A.
Comments: AIDA is a business marketing strategy consisting of 4 elements: Getting the **Attention** of the audience, developing an **Interest** in the message, creating a **Desire** for the message, and encouraging the audience to take **Action**. This should be considered when developing security awareness and training programs.

2. In order for a security plan and associated policy to be effective, it is important to have buy-in from all areas except:
   a) Executive leadership
   b) IT Department
   c) People outside the organization
   d) Employees and other users

Answer: C.
Comments: Although buy-in is essential throughout the organization, the success security plan and policy does not rest on the cooperation of outsiders.

3. Most surveys of computer security losses show that actual losses are greatest from:
   a) People inside the organization
   b) Outside Hackers
   c) Viruses
   d) System Malfunctions

Answer: A
Comments: In *Site Security Handbook, RFC 2196*, Fraser wrote "There is a great deal of publicity about intruders on computer systems; yet most surveys of computer security show that, for most organizations, the actual loss from 'insiders' is much greater."

4. Of the items listed below, which is not a NIST recommended step to establish an effective security training program?
   a) Identify program scope, goals, and objectives.
   b) Secure financial backing.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

c) Identify target audiences.
d) Evaluate the program.

Answer: B
Comments: In the NIST publication *Generally Accepted Principles and Practices for Securing Information Technology Systems* the following are recommended steps to establish an effective security training program:

1. Identify program scope, goals, and objectives.
2. Identify training staff.
3. Identify target audiences.
4. Motivate management and employees.
5. Administer the program.
6. Maintain the program.
7. Evaluate the program.

5. Knowledge differs from information. Which of the following statements is not correct?

a) Information does not always lead to understanding
b) Information goes beyond the facts, connecting and explaining them.
c) Knowledge, not information, best contributes to empowerment.
d) Knowledge further refines information.

Answer: B
Comments: Andrews & Herschel wrote, "Information does not always lead to understanding. In contrast to information, knowledge goes beyond the facts, connecting and explaining them."

True/False

1. True/False: Applying communications theory and strategies can be effective in increasing organizational buy-in for an information security program.

Answer: True
Comments: Information security officers must take into account the need for effective communication strategies when soliciting organizational buy-in.

2. True/False: Awareness efforts differ from training in that the former is more formalized and structured.

Answer: False
Comments: Training programs are usually more formalized and structured than awareness programs.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

3. True/False: Denial of Service attacks which use email hoaxes exploit a lack of understanding on the part of users. Information security awareness and training programs can effectively combat this.

Answer: True
Comments: Awareness and training programs can empower users and provide a needed layer of defense.

4. True/False: The overarching goal of security awareness programs is to move people to care about security.

Answer: True
Comments: Where security training is concerned with teaching people the tools and procedures to follow, security awareness programs seek to build organizational commitment and support.

5. True/False: Security professionals should distance themselves from the rest of the organizational community in order to maintain a high level of professional respect.

Answer: False
Comments: Security professionals need to demystify themselves and their profession so as to become a part of the organizational community, and concurrently help people understand their own responsibilities within that same community.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**