Global Information Assurance Certification Paper

Security Awareness: Preventing a Lack in Security Consciousness

Katherine Ludwig
SANS Security Essentials
GSEC Practical Assignment
Version 1.2d

With the ever-changing world, ever-changing technologies and ever-changing programs coming into existence that make our technical world more exciting and productive, so too does the security world change. Of course, along with these advancements, new holes, bugs and exploits are found by unscrupulous and unethical individuals to exploit for their own gain, manufacturers of security products struggle to keep up with fixes, patches, and new releases in an effort to keep up-to-date with the surrounding market and, not at the least, security professionals grapple everyday to overcome a lack of training, knowledge, support and compliance from the general populace of their company. Bruce Schneier, CIO of Counterpane Internet Security Inc., "Computer security is a 40-year-old discipline; every year there's new research, new technologies, new products, even new laws. And every year things get worse."

Many surveys are executed in an effort to grasp the extent of the security problem we are facing. Following is an excerpt from Computer Security Institute's web site (http://www.gocsi.com/prelea_000321.htm):

> …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.

- Eighty-five percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- Sixty-four percent acknowledged financial losses due to computer breaches.

- Forty percent of respondents detected system penetration from the outside (only 25% reported system penetration in 2000).
- Thirty-eight percent of respondents detected denial of service attacks (only 27% reported denial of service in 2000).
- Ninety-one percent detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems). Only 79% detected net abuse in 2000.
- Ninety-four percent detected computer viruses (only 85% detected them in 2000).

The numbers above, taken from the 2001 Computer Crime and Security Survey, show some startling and horrifying trends in computer crime. These numbers are only projected to increase.

Although there are numerous challenges facing today's Information Security professional, this paper will focus upon only one … and perhaps the toughest: How to

win over the company's employees to a secure work style by means of a good Security Awareness program.

As stated on Security Awareness Incorporated's web site (http://www.securityawareness.com/):

> There are numerous controls IT professionals can implement to safeguard electronic information from unauthorized users. But it's the authorized end users that possess the IDs and passwords to access that data giving them the ability to print it, share it, alter it or delete it. If they are careless with or choose weak passwords, casually discard confidential printed reports in the trash, prop open doors to secured areas, fail to scan new files for viruses, or leave back-ups of data unsecured, then that information remains at risk.

A Security Awareness program is probably the most important weapon in the Information Security professional's arsenal. A company can have every security product known to the industry, but these products will be worthless in the face of the one user who disregards or is not even aware of the proper security procedures. This includes something as simple as keeping their password secret.

Many companies espouse a Security Awareness program. But what does that mean?

- A ten-minute speech in employee orientation?
- A small paragraph in an employee handbook?
- A pen or magnet with a security motor labeled on it?
- A brochure that is given in the employee new-hire packet?
- A poster in the hallway showing a threatening situation or message…. with a title of "Be Aware"?

Well, while all of these things individually are commendable, it is not until each and every person realizes that what they do, how they do it and why they do it impacts, not only the safety of the company's assets, but also impact the assets of individuals around the world, that a Security Awareness program is successful. In the following, we will touch upon some characteristics of a successful Security Awareness program.

A Security Awareness program should:

- Educate and inform employees, at the very minimum.

  From corporate management on down, the importance of data and information security needs to be conveyed. Security policies, standards, guidelines, and procedures achieve their maximum effectiveness when steps are taken to ensure that all employees fully understand the reasons underlying their significance and the specific security-related requirements to their particular duties. Employees

should be directed as to where they can locate their company's written policy, standards, guidelines and procedures.

- Achieve a workable balance between security and productivity.

  As referenced in the Computer Security Handbook (authors Hutt, Bosworth and Hoyt), a balance needs to be struck between information security and productivity. When information security programs overextend themselves, they become burdensome and impede the productivity of the user community. On the other hand, where security measures are nonexistent or too lax, information systems and data are vulnerable to disruption, modification or destruction.

  Companies need to establish the level of risk they are willing to absorb versus the intensity of the exposures they wish to close, while also ensuring that their employees have the necessary access and authority to perform the business objectives. Striking a balance between these two extremes is a difficult task to accomplish. (John D. Johnson, Infosec for Dummies Part II, http://securityportal.com/topnews/infosec-dummies3.html)

- Communicate to individuals the importance and general concepts of security, without inspiring boredom (Computer Security Handbook (authors Hutt, Bosworth and Hoyt)).

  Security Awareness programs should include many realistic examples of security requirements and breaches. If Security Awareness programs rely on strict presentation of facts, they will hit a dead end. The intended audience will tune out the information and all will be for naught. The program must appeal to the individual's imagination, emotion, and sense of responsibility and logic. The program should utilize real world, high profile examples of security stories. In the recent past there have been many headliners that most people have at least heard of: "LoveLetter Damage Estimated at $10 Billion", Los Alamos Loses Top-Secret Hard Drive", "Microsoft Security Woes Continue", and so on. Use these headliners to raise the employee's Security Awareness levels as they have raised the Security Awareness levels universally. Remember that the end goal is for the person to be left with a desire to be secure and a better understanding of how to do it. Security is everyone's responsibility!

- Bridge the "cultural divide" between the Information Security team and the remaining support teams/populace of the company.

  Regardless of whether the medium to distribute the Security Awareness program is a lecture, a poster, a video, a brochure, or any other media, the verbiage utilized in the Security Awareness program needs to be geared toward its audience.

Every organization is comprised of specialty departments that play a specific role in obtaining the company's business objectives. … (The) more specialized the department structure, the greater the communication gap. … When communicating with people of other disciplines, it is important to use their language if you want to get your point across. (Jay Heiser, "Cultural Divide", Information Security, May 2001.) The presenter of the program needs to be sure to avoid using technical security jargon that may confuse and distance the employees.

- The mindset of the individual must be addressed.

  We all know quite a lot about physical security. If you are a woman, you know to lock your doors, keep your car keys in hand, stay alert, don't open the door to strangers, and be aware. Children are taught to not talk with strangers, don't leave school with someone other than their parents, don't swim directly after eating, don't run up to a strange dog. Not following these precautions can result in direct physical harm to you. Those who care for us drum physical security into our heads from the time we are first able to communicate. When adverse things can happen to us personally, we tend to take action to ensure that they do not. Do you realize that these same things apply to your intellectual property, as well as your company's intellectual property?

  As Information Security professionals, it is our responsibility to ensure that the employees can personalize the intellectual security concerns of their company. "What you do, how you do it and why you do it" applies to them personally as well as to their company.

  For example, an employee at a financial institution may bemoan the fact that they have to change their password every 45 days. So they write it down on their desk, stick it on a post-it, display it for the world to see. They are basically following their company's specific security policy requiring them to change their password on a frequent basis. However, perhaps because they do not fully comprehend the implications of WHY they are required to do so, they flaunt the authority and "tell" it to everyone. On the surface does this hurt anyone? No, not intentionally. But, then his or her password is stolen and someone in a "black hat" (a.k.a. bad guy) hacks into the institution and steals everyone's money. Now think of all of the people that were left unsecured by the one person who didn't safeguard their password. Now, if the clerk had money in their own institution, would they have been more safety conscience? Maybe, maybe not. This depends on how security aware the person was. A major reason for the lack of threat awareness by people is the failure to grasp what can be lost through security breaches. (John D. Johnson, Infosec for Dummies Part II, http://securityportal.com/topnews/infosec-dummies2.html)

All Security Awareness programs, for both physical and intellectual property, need to be constantly broadcast in a manner, which allows the individual to personalize the danger. Walk in a dark parking lot in the bad side of town, and you may be mugged or worse. Don't practice good security at work and you, or other actual people just like you, can suffer financial harm. Only when the message is personalized, will it have a chance at being received and heeded.

- Social Engineering should be addressed in depth.

  Let's face it, if there were not an element of humans who desire to do wrong, we wouldn't need much security. But there are and we do. Social engineering is a broad term that describes a method the 'bad' people use, with great success, to gain information to do harm. Basically social engineering is misrepresentation. It relies on lies, bribes, falsehoods, and seduction to trick honest or, at least marginally honest, people to reveal information.

  Lying is a very obvious ploy. In a corporate office, an individual in a suit walking assertively down the hall has every right to be there. Or does he? In a computer room, a person in coveralls with a briefcase full of equipment is supposed to be working on the computer or phones…right? The person on the phone who says that they are the boss, a manager, a helpful vendor, or anything else like that … are they? People naturally assume that all around them are honest, decent hard-working people just like themselves. Most people assume what you see is what you get. Security Awareness programs need to impart the knowledge that, unfortunately, this is not true.

  Impersonation of authorized personnel also falls under social engineering. The phone system is widely used in this effort. Criminal and unethical minds use the phone system to call employees to request logon IDs, passwords, privileges, company information, as well as a wealth of any many other types of information. We are programmed, if you will, to serve the customer in all things and we want to help make our customer happy. So, many times, these phone calls work.

  Seduction (yes this happens in real life, not just the movies!), extortion and blackmail are more types of social engineering that unscrupulous individuals can and do use.

  - Password protection.

  Individuals should come away with an understanding of why their password is so important, why it needs to be changed frequently, and why it must remain secret – known to no one but themselves. It is not only to protect the company; it is to protect the person. This ties back to being able to personalize the security threat.

> Do you want anyone to know the pin number of your ATM card? What about your credit card number? Well, you don't want anyone to know your work password for the same reason…prevention of identity theft. It would be terrible if someone gained access to your ATM card and pin number and stole your money. Wouldn't it be awful if someone could damage your company's major systems while leaving your ID in all of the audit logs, thus implicating you in the crime? This is just something to think about.

The above topics are just some of the elements that, if covered, will assist in your Security Awareness program in being successful. There are so many aspects of Security Awareness that it would be impossible to cover them all.

The firm point that needs to be made is that without an effective Security Awareness program in place and functional, odds are that the Information Security team's hard work at developing and implementing the wonderful tools to protect your company's assets, the extensive time put into developing and publishing the policies, standards and procedures, and all the other hundreds of things that go into our day to day lives, will be virtually worthless.

Sources Cited/Referenced

Bruce Schneier, “Network Security: It’s not about the technology”, 5/1/01, URL: http://www.itworld.com/AppDev/1310/CIO010501et_pundits/

Computer Security Institute [WWW page].
URL http://www.gocsi.com/prelea_000321.htm

Security Awareness Incorporated [WWW page].
URL http://www.security awareness.com/

Arthur Hutt/Seymour Bosworth/Douglas Hoyt, Computer Security Handbook, Third Edition, 1995

John D. Johnson, “Infosec for Dummies Part II”,10/29/99, URL: http://securityportal.com/topnews/infosec-dummies2.html

John D. Johnson, “Infosec for Dummies Part III”,11/04/99, URL: http://securityportal.com/topnews/infosec-dummies3.html

Jay Heiser, “Cultural Divide”, Information Security, May 2001