GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Douglas Alred
July 18, 2001
SANS Security Essentials
GSEC Practical Assignment
Version 1.2e

Awareness, A Never Ending Struggle

The setting is a large federal government owned facility operated by a major contractor
with quite a number of sub contractor personnel also on site. All contractors and sub
contractors are required to attend computer security awareness training by their federal
customer. Training rosters are signed and entered into tracking to document that yes, all
personnel have received the required training. This may satisfy any government and
company requirements but the real test occurs every day. Will employees follow the
guidance they have been given in awareness training? Below are some example scenarios
that could take place.

  1.   Does the desktop user open a suspicious e-mail attachment?
  2.   Does the network administrator conduct intrusion checks?
  3.   Does the janitor ensure no one tailgates into the building before the door shuts
          when entering or existing the computer center?
  4.   Does the Finance Department share passwords for database access?
  5.   Does the high level manager think it's necessary for annual awareness
          training?

The number of things that can result in a computer security incident can go on
indefinitely. So how do we has computer security professionals assure ourselves that we
are secure. No matter how many technically advanced products we use or how large our
security budget is it all comes down to the fact that security depends on people and their
awareness.

According to Webster's Collegiate Dictionary **Awareness** is the act of having acute
sensitivity or knowledge of something which one would exhibit vigilance, observance
and/or alertness.

Ok, so what are we to be aware of? There could be many answers to this question but I
would answer that we should be aware of what we are protecting and what are the risks,
threats, and vulnerabilities associated with it.

Information

 No wonder that "Computer Security" is sometimes referred to as "Information Security".
After all it is the information that we are striving to protect. We wouldn't be very happy if

we had a computer to be lost or damaged but for 99% of us the loss of the computer would be <u>nothing</u> to the loss of the information it contained.

Awareness is necessary in providing information protection. It's necessary to protect the Confidentiality, Integrity and Availability (CIA) of information. CIA is the foundation that an information security program should be built on. The information owner needs to make a decision of how much security emphasis should be placed in these areas. How much privacy or secrecy is necessary? Is it necessary for the information to always be accurate? Is it necessary for the information to always be available immediately at all times or are delays acceptable? To answer these questions the information owner needs to be aware of how important the information and access to the information is. Once that's determined then the awareness of threats, risks, or vulnerabilities need to be considered. Awareness again is the most important tool in recognizing what these threats, risks or vulnerabilities are.

Scenario One – Does the desktop user open a suspicious e-mail attachment?

This user has been through the facilities computer security awareness training and remembers that due to the possibility of e-mail attachments containing viruses she should not open any attachments from unknown or unsolicited sources. She also has anti-virus software, which she can use to scan the attachment. If a virus is detected she can delete it and save herself some frustration and keep her information secure. If not for participating in her facilities awareness program she probably would not have recognized the possible threat that viruses via e-mail attachments present. She would not have been able to analyze the risk to her information of opening this attachment. Also, she would not have been able to eliminate the vulnerability to her system. In this case the objective has been met. The awareness information that was presented helped prevent a possible problem. The awareness program has passed the test.

According to the 4th Edition of the Computer Security Handbook:

> An organization's staff is the most cost-effective countermeasure. They are
> generally the first to be impacted by potential security incidents and their
> compliance with security policy can make or break a security program. A staff
> that is aware of security concerns can prevent incidents and mitigate damage when
> incidents do occur. Given the importance of the staff as a security control,
> awareness is therefore the most important part of an organizations security
> program. Experts recommend that 40 percent of an organization's security
> budget be spent on awareness measures. (Rudolph, Numkin, Warshawsky, 29.1)

Some organizations may tend to focus more on other ways of protecting their information. They may tend to spend funds on items such as firewalls and network scanning tools, leaving very little funding for other things such as awareness training or education.

Scenario Two - Does the network administrator conduct intrusion checks?

The administrator has the tools that should enable him to conduct network scanning. He can scan for vulnerabilities within the network and threats from outside. These internal vulnerabilities could include workstations and servers not properly configured which could be easy targets for the outside threat of denial of service attacks or hackers attempting to gain access to information. The administrator has taken the facility's required computer security awareness training but it is a basic generic presentation that does not go into advanced technical concepts that would help him. While the site has spent quite a bit of funding on getting the proper tools for protection and is in compliance with its customers' awareness requirements there still exists a vulnerability. There have been several patches and updates to the administrator's tools that he is unaware of. The facility's awareness program has not worked well with keeping up with technical changes. There are things happening on the network that the administrator doesn't know to look for or recognize. The network is vulnerable. To stay on top of the game people in technical areas such as system or network administrators must constantly stay aware of the latest threats, risks and vulnerabilities. Technology and the software (good and bad) that goes with it changes daily. This is one reason a good awareness program would include constant updates on the latest topics. In this case the awareness program has failed.

There are some very good awareness sources that are a must. They include but are not limited to:

- Computer Incident Advisory Center (CIAC)
  http://www.ciac.org/ciac

- National Infrastructure Protection Center (NIPC)
  http://www.nipc.gov/

- National Security Institute's – Security Resource Net
  http://nsi.org/compsec.html

- Carnegie Mellon Software Engineering Institute (CERT)
  http://www.cert.org/

- SANS Institute
  http://www.sans.org/newlook/home.htm

Scenario Three - Does the janitor ensure no one tailgates into the building before the door shuts when entering or existing the computer center?

The janitor has been allowing people to enter by not ensuring the door is closed after he enters or exits. No one has entered that was not authorized but it could happen. This may happen due to the janitor not paying attention or thinking anyone walking in behind him is no big deal. With the proper awareness training the Janitor might pay more attention and be concerned if anyone attempted to enter without proper approval. Even though the janitor received the facilities' annual computer security awareness training the act of physically protecting the facility may not have sunk in. In this case the awareness program has failed.

Perhaps in addition to the required training there should have been other awareness tools used presenting information in different ways or perhaps stressing different things. The janitor would not necessarily need to know or even be interested in some of the awareness information that a desktop user or a system administrator would need to know. Below are some examples of mediums that can be used to present awareness information.

- Web Based Training (with or without quizzes)
- E-mail bulletins (such as CIAC Vulnerability Notices)
- Handouts (e.g. company computer policies, tips on identifying incidents, etc.)
- Videos
- Awareness Meetings
- Short Awareness Presentations (Piggy backing at the end of a Safety Meeting, etc.)
- Billboards, Posters, Fliers, Magnets
- Public Address Announcements
- Newsletters
- Warning Banners

Scenario Four - Does the Finance Department share passwords for database access?

The Finance employees all have the same need-to-know for their database so their manager has allowed them to use a common password to access their server. This is against facility policy and is also covered in the awareness training. The awareness has failed in this case. Even though the users have a common need-to-know there now exists no audit trails and if someone from the outside were to obtain the common password they could get to all information on the server. Why did this happen? Perhaps the awareness training did not stress why passwords should not be shared and the possible resulting damage. Although the outsider threat has grown tremendously over the past few years the insider threat is still very real. A careless or disgruntled employee could wreak havoc on a server. If passwords are shared not only could the person access their own data but everyone else's also. Another possibility is that the policy and the awareness training were ignored for the sake of convenience. With the matter of convenience perhaps the training should have covered consequences for employees that ignore policy. This next scenario also touches on convenience.

Scenario Five – Does the high level manager think it's necessary to take annual awareness training?

One of the managers at the facility thinks it should not be necessary for everyone to take the required training. The only time he uses a computer is while on travel he uses a laptop for e-mail communication with his secretary and he really doesn't have time for awareness training. When at work his secretary does all the computer work for him, including his e-mail. The computer security department in this case has to sell the product (computer security awareness) and show the manager how the awareness training will benefit him. Since he uses a laptop for e-mail when traveling information on the vulnerabilities of portable computers and viruses are presented to him in a way that makes sense to him at not only a management level but now as a responsible computer user. It may have taken some extra work on the part of computer security personnel but the awareness training will pay off in this case.

Conclusion

I've given five examples of everyday events. These events and many, many others do happen every day. In some of the examples the awareness training paid off and incidents were avoided. In the other cases more awareness or awareness presented in a different form may have prevented problems. The successful presentation of computer security awareness is a constant struggle. It has to be presented in many different ways to reach and influence everyone that is necessary to ensure the best security possible. A computer security department has to be flexible in how the awareness is presented and constantly be ready to add or change this awareness information as the needs arise. I hope that by using the five examples I've been able to emphasis some key points to any successful awareness program.

1. Sell the need for awareness to management! Not only for the company or facility as a whole but for the different levels of employees; management, technical, and non-technical.
2. Obtain sufficient funding for the awareness program!
3. Present the awareness to the different level or types of employees in ways that will have meaning for their specific job duties!
4. Cover all the different security aspects (administrative, technical, information, personnel, physical, etc.)!
5. Have several different types of medium to use for communication of the message!
6. Update the message(s) to stay current with technology and events!
7. Analyze the program and the results, make changes if necessary!!!

There will always be room for improvement. The challenge and struggle to have a successful program will always be there. There will always be threats, risks, and vulnerabilities. But the Strong will survive and a solid awareness program is the key

to that survival.

Citations

Rudolph, K, CISSP, Numkin, Louis, and Warshawsky, Gale,Computer Security
Handbook, 4th Edition, Chapter 29 (Draft). July 11, 2001
URL: http://nativeintelligence.com/awareness/chap29-1.asp

Pethia, Richard D., Testimony before the Senate Judiciary Subcommittee on
Technology, Terrorism, and Government Information, "Removing Roadblocks to
Cyber Defense". July 11, 2001
http://www.cert.org/congressional_testimony/Pethia_testimony_Mar28-2000.html

Computer Associates' Virus Information Center Guidelines for Users Who Find a
Virus http://www.ca.com/virusinfo/managing.htm#sec36

Santana, Arthur, The Washington Post, Thieves take more than laptops. November 5,
2000. http://www.washingtonpost.com/wp-dyn/articles/A9633-2000Nov3.html

National Center for Education Statistics, Safeguarding Your Technology, Chapter 10,
Training: A Necessary Investment in Staff.
 http://nces.ed.gov/pubs98/safetech/chapter10.html