Security Awareness Training Quiz - Finding the WEAKEST link!

David Sustaita

GSEC Practical Assignment version 1.2e
Security Awareness Training Quiz - Finding the WEAKEST link!
David Sustaita
August 13, 2001

Introduction

It is an old maxim that a chain is only as strong as its weakest link. This assumption has long guided the understanding of computer and network security. As a result of this, organizations need to employ not only a security overview but also put in place a testing mechanism to make sure their employees understand the basics of computer security.

The security overview should be designed and implemented to help end-users get better acquainted with the network environments that they work in. A basic framework should be put in place to ensure the end users will be able to understand the concepts. Different tests may be catered around more technical groups if necessary, and the testing mechanism should be mandatory to determine if the end users understand the concepts covered.

Although there are a great number of companies that employ the use of some sort of security awareness training, many still have not realized the need for training at all and this should not be acceptable. With the basic training some organizations provide, many users just go through the motions to complete the course or review. Along with a solid foundation, end users need to be tested to see if they have successfully understood the information that was taught. This testing system is vital if an organization is serious about it's security awareness training. The test or quiz (if passed) should generate a printable certificate with the end user's name and a date stamp. The end user should sign and give it to their supervisor and have another copy placed in their HR file. The certificate ensures that the end user has at least a basic understanding of security. The testing mechanism demonstrates the organizations' motivation to educate the end users so as to eliminate superfluous security risks.

Why Security Awareness?

> **"Security Awareness is fundamental to all activities that protect computing resources."** -Native Intelligence, Inc. 2000

Actually, the only way to guarantee that you have a secure system is to turn it off or just unplug it This is not an acceptable alternative in our high tech world that depends on information systems daily. Companies use computer systems and resources everyday to complete mission critical tasks and these companies need to understand the risks of allowing end users that are not aware of security, operate their systems and to begin defending themselves from preventable threats.

> **"Security apathy and ignorance are the biggest threats to computer systems. . . . And the best way to achieve a significant and lasting**

improvement in computer security is not by throwing more technical solutions at the problem -- it's by raising awareness and training and educating all computer users in the basics of computer security." - Native Intelligence, Inc. 2000

The Creation Process

Ok, so now that you know that you need a test/quiz… where do you start? The first thing you need to do is start at the very bottom, the foundation of the training material. It is imperative to already have in place a good security awareness training program. Once this is done, you need to determine the most general areas of security covered in training then break down the topics in more clearly categories. And since your employees run into different issues daily, you also need to determine what issues and threats your company is facing on a day-to-day basis and include these in both your training and testing. A great way to get a feel on what direction your awareness training should go in is to also gather information from both managers and end users and get a feel for what they are interested in learning about. Remember, there is NO such thing as a stupid question so keep the information gathering at the broadest level at first so as to get an adequate amount of information to build a solid foundation for your training and testing. Once you have gathered enough information you can start to categorize the information into subject areas like password management, social engineering, and security. Now that you have all the information broken down into different subject areas you will be working with, you will need to start sifting through the information using a filtering process that takes the information and puts into a simpler base from which you can draw out two parts, a question and an answer.

Test Questions

Questions can be written in different forms. An example test may contain 20-25 questions consisting of 10% true / false questions and 90 % multiple-choice questions or any other combination therein. Questions should always be laid out in a readable format. They should not try to trick the end user but help them to understand the importance of the subject material. Answers and questions should be basic enough for the end user to retain so as not to lose the purpose of the testing process. If the end user retains the information from the training, then they should have no problems passing the test, and after all that is what we want as managers - informed security conscious users.

Now What?

Now that you have come up with a set of questions and answers, you need to determine the best method of creating and implementing the test. We knew that we wanted to deploy a web based testing mechanism so we experimented and evaluated the different web based technologies around to determine what we would best be able to utilize. Cold Fusion best met our needs but it may not be as useful to another organization so it is best that you evaluate what best fits your organizations needs. Once the technology was selected, we built a Cold Fusion application that was used to deploy the

training and the testing mechanism. We first have the end-users start at an authentication (login) page where they use their LDAP (Lightweight Directory Access Protocol) alias to login. Once the user is authenticated using a username and password, the application gets and passes, through an LDAP Query, the user's name to the page where the test resides as a hidden variable. Other hidden variables that are also passed are the end user's department and the date on which the test is taken. Other web languages can be used but Cold Fusion was selected because of its connectivity to our LDAP and SQL servers. The SQL server is used to store each user's attempt at the test and whether they pass or fail in a central database. The end user's name, department, whether they pass or fail, and the answers they submitted on the test are all stored in a database for historical reference. Managers and supervisors can later query the database to find information about department statistics, end user statistics, and other information like how many end users miss a particular question that may lead to changes to the training and testing process itself.

The Federal Information Systems Security Educator's Association addresses the need for "Awareness Quizzes" and takes a great approach for providing a mechanism for testing:

> **"The purpose of awareness is to make your customers aware of threats, vulnerabilities, corporate policy compliance issues, etc. Your goal is to change behavior and make the customer knowledgeable of their role in protecting your company's/organization's information You WANT them to get the correct information, even if they select the wrong quiz answer.**
>
> **The format is as follows: Provide the question. Provide the multiple-choice answers. If the customer selects the correct answer, that html-linked file informs them, "Congratulations! That was the correct answer." If the customer selects an incorrect answer, that html-linked file informs them, "That was not the correct answer. The correct answer is ..." (and provide information as to why it is the correct answer).**
>
> **We found it useful to provide an on-line certificate of awareness at the end of the quiz. Instruct the customer to print it out and enter their name on it. I have found that people LOVE to have certificates of awareness and certificates of training. I've seen them displayed in cubicles at many office locations. I've received E-mail messages from satisfied customers complimenting Information Security management on the awareness quiz and its usefulness."** -Federal Information Systems Security Educator's Association. FISSEA Newsletter - Feb. 2000

The Review and Update Process

Information Technology and the issues that it brings to the table are changing on a daily basis. It would be impractical and almost impossible to make users retake the training and take another test each time some new product comes out or when systems are updated, but it is important to have some type overview at least on a yearly basis. This could be done by just altering the data in the training to reflect changes in the systems used by the organization. Also since new issues come up often like new threats or something like hoaxes which also waste valuable resources like manpower and bandwidth, a yearly review is a great time to inform end-users of these new issues or situations.

San Quinton

What a better place to look at security than a state prison. The San Quinton State Prison requires its employees to go through information security awareness training. This is done by having its employees go online to their website and go through the training there or they can also download the training manual from their website in an Adobe format as a handbook which can be printed out and looked over at anytime. The website also provides a pool of questions for the employees to go through as a quiz and which are updated monthly and the answers are found within their handbook they printed or online. Although it is not a required quiz it is still a good idea and the fact that they change the subject matter so the employees understand a broader area of security is also good as so the employees do not just memorize certain key facts.

'Certified' Security Awareness

Once the end-user goes through our online security awareness training, and pass, they get a training certificate to show they have completed this requirement. We have decided that the Security Awareness Training Certificates are valid for one year from the test date and the questions are changed also on a yearly basis so no one takes the same test twice. Once the certificate is coming upon its expiration date the end-users just logs back into our system, reviews the information, and takes the test again. Since this is done on a yearly basis most users do not mind having to complete the training and testing process again and we have received favorable responses indicating that the updated information was found to be very useful.

Oracle

Oracle has taken a huge step in its security awareness training program. Oracle's Global Information Security Services employees all have to go through security training….. with a twist. Depending on the end-users position, they have broken the training down into three groups, one for the "Average Employee or Human", one for a "Sys Admin / Techie Engineer" and one for a "Manager / Facilities Personnel". The training is catered around the environment that the employees are in. The Average Employee training is less intensive whereas the Sys Admin training is much more detailed and also deals with many more tools that the average user never has to deal with. The idea behind the separation is good but they still do not have any type of testing

mechanism in place to determine the basic understanding of security that each employee has.

CSI Survey

The Computer Security Institute recently published the 2001 CSI/FBI Computer Crime and Security Survey and it contained some very interesting statistics:

> **Ninety-one percent of surveyed organizations 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).**

Just in these two findings, companies must realize that they need to do everything they can to not only require security awareness training but also require the testing of those employees to determine if they have actually retained the information they were taught and to MAKE SURE they have a basic understanding of information security. Organizations all have mission critical information that needs to be protected and this is done not only through physical security but also performed by security of the systems that interface with it and the operators of both the systems and resources that interact with this information. If the end-users that deal with this information do not have at least the basic understanding of security, all the other means of protecting their information and systems are moot.

Conclusion

Computer crime is on the rise and has increased every year since computers were first used. The government is doing what it can to combat these issues but it is up to each organization to make sure that it is doing ALL that it can to ensure it is acting responsible in our high tech world. In the world system that organizations now work in, it is more of a threat now than when companies only did business with companies across the country much unlike doing business now around the world. Costs incurred dealing with responses to security related issues over the past year have been caused by both outside and inside sources and must be headed off through responsible computing. This can only be done by making sure organizations are running both efficient security awareness

If companies take strategic measures in creating a training program like that of the SANS institute in it's creation of the SANS GIAC program, and not just throw together a few power-point slides to check the training off their list, it will be evident that the IS department is serious about awareness training. With such a program in place, the creation of a testing mechanism should not be a problem and will benefit all employees that go through the training and testing and ensure management that it is doing everything it can to secure its systems at the basic end-user level.

References

1. Federal Information Systems Security Educator's Association. FISSEA Newsletter - Feb. 2000
URL:http://www.sans.org/infosecFAQ/start/awareness.htm

2. Native Intelligence, Inc. Security Awareness
URL:http://nativeintelligence.com/awareness/index.asp

3. California Dept. of Corrections, San Quinton State Prison - Information Security Awareness.
URL:http://www.cdc.state.ca.us/ISU/AwarenessSecurity%20Awareness.htm

4. Oracle's Global Information Security Services - Building Good Security at Oracle... what do YOU need to know?
URL:http://www.mfgraffix.com/oracle/infoprot/

5. Computer Security Institute, CSI/FBI Computer Crime and Security Survey 2001.
URL:http://www.gocsi.com/prelea_000321.htm

6. Sans Institue, GIAC Security Essentials Certification.
URL:http://www.sans.org/giactc/levelone.htm