Global Information Assurance Certification Paper

GSEC Practical Assignment Version 1.4c

Author: Salman Ashraf

Date: February 08, 2005

Organization Need and Everyone's Responsibility

Information Security Awareness

Table of contents

1 Introduction

Information is considered lifeblood of a successful and profitable business and employees of the organization work as veins to pass this information through. Confidentiality, Availability and Integrity of information are then directly related with employee's behavior towards information. Most companies think information security is a technical issue and do not consider involvement of employees in ensuring continuous security of the information. Organizations may have components of information security awareness program but without proper management of the needed resources, they will not be able to complete it properly and continue to be successful. Identifying and bringing together all available components to develop an effective information security awareness program can be a difficult and overwhelming task.

This document mainly focuses on the needs of an information security awareness program. The document discusses the techniques and methodologies that can be used to implement it with proper involvement and motivation of the staff. Information Security awareness methodologies are a vital issue and play an important role in meeting the intended goals of an organization. This document discusses the methodologies and what to take into consideration while implementing those methodologies. Along with methodologies implementation of an information security awareness program is a main task and gives final result. The paper also discusses implementation of an awareness program and some of the obstacles in implementation. It seems very difficult to involve employees and busy managers in such programs which are not related to their job. This document describes the importance and the association of employees with information security awareness program, and motivational factor to attract employees to be responsive to this program. This is required and is the responsibility of all members in the organization to protect the information assets.

2 Brief about Information Security Awareness

Information Security is the protection of information in opposition to fault, disclosure and manipulation.

It is commonly accepted that the majority of the security violations are due to human interaction rather than technology fault. Yet, companies depend and grant a lot of consideration to technology and usually forget participation of human beings in the system. Usually organizations use best of the best products and technology for the protection of information and infrastructure. They ignore human's contribution and role in securing organization assets. Actually companies make this mistake and relate information security with the products and technology although it is a process which needs human interaction and involvement. There is no such thing as 100% security but we try to maximize its level through an awareness program and human involvement in the process.

A simple definition of the three security pillars is as follows. If anyone of them is missing then it's a flaw and is against the information security measures.

Confidentiality: It means only authorized people can see information e.g. you are the only one authorized to see your bank statement.

Integrity: It ensures that information has not been changed either in transit or while in storage. It means only authorized people can change the information e.g. you can see bank statement but not authorized to change it according to your wishes.

Availability: It means information is available when and where it is needed e.g. you can get money from ATM machine when you want to buy things.

Information Security Awareness is user's education and awareness to handle information security threats and minimize their impact. Awareness program basically focuses attention on information security issues like confidentiality, integrity and availability. It highlights the importance of these factors, their role in business and finally concentrates on how to behave with them in a confident way.

"Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly."[1]

Information Security awareness is a method used to educate people in the organization. It highlights the importance of information, threats to that

[1] National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program

information and staff's contribution in implementing policies and procedures for the protection of information. Awareness program is an attempt to change the behavior of employees towards systems and processes in the organization. It teaches what needs to be protected, against whom and how.

3 Information Security Awareness is a Business Need

In today's business environment most of the companies rely on electronically exchanged information. It is a requirement of all the departments to produce and pass information across different departments in a quick and secure manner to support their business decisions. Information plays an important role in making decisions. Therefore commercial companies and even the government departments have different classification of data based on its importance and use.

Business success depends upon continuity of operations and information provided to the business processes by information systems. The growth, excellence and efficiency of the business could be damaged due to the threats and misuse of information. Therefore, awareness program basically helps, set measures and educate users on how to behave and get benefit out of information without jeopardizing its confidentiality, integrity and availability.

The employees are the primary users of the information. A lack of awareness and mishandling of information could expose this information to competitors or get corrupted. If this information is freely available the following could be some of the impacts on the company and its business functions:

- The information available easily can be used by competitors to design strategies and launch new products with more features
- The company's credibility can be affected from this disclosure
- Customer confidence can be lost
- Help competitors to gain more share in the market
- Suppliers and partner would be conscious to deal with the company
- Non compliance to government and industry laws and standards
- Employees will lose trust and will look for other opportunities

In today's competitive business environment to have a good reputation in the market and legal compliance is a major concern. Suppliers, partners and even clients ask proof of information security before making any transaction. They want to make sure that all the information given to the company will be protected and will be used only for the purpose it is provided.

Therefore need of successful and responsible organization is to have well written security polices and procedure, run information security awareness

program on a continuous basis and be conscious in protecting its information assets. Implementing a strong information security awareness program can be a very effective method to protect critical business secrets and it will help employees to understand:

- ☑ ***Why*** they need to take information security seriously
- ☑ ***What*** they gain from active participation and support
- ☑ ***How*** a secure environment helps them complete their assigned tasks

4 Information Security Awareness Goals and Objectives

As we all know people are the weakest link in the chain and are the source of many information security breaches within the organization. Before demanding information security, employees should be conveyed the importance of company's information and criticality. An educated and aware user is the foundation of a secure and reliable business environment.

Dealing with information security threats and incidents is not a technology issue but people's behavior. It is a critical factor to have a successful and effective information security program that will modify the behavior of employee's dealing and interacting with company's policies and procedures.

Usually IT or Security department is considered responsible for the security of information assets. It is a misconception which has to be communicated among employees that the IT department is not the only one responsible but Information security is everyone's responsibility. Information Security is everyone's responsibility and at any level of the hierarchy.

Information security awareness program helps in minimizing the cost of security incidents, helps accelerate the development of new application systems, and helps assure the consistent implementation of controls across an organization's information systems.

The primary and foremost objective of any awareness program is to educate users on their responsibility to protect the confidentiality, availability and integrity of their organization's information.

One of the objectives of an awareness program is to convey simple, clear and presentable message in a format that is easily understood by the audience.

The awareness program's objective is that users understand not only how to protect the organization's information, but why it is important to protect that information.

Awareness program's goal is to get users attention on information security

policies and increase awareness level on all security controls and practices in the organization.

One of the goals is to create a security culture across the organization and keep on reminding employees about its importance and their contribution in that.

> "Continuous improvement should always be the theme for security awareness and training initiatives, as this is one area where "you can never do enough.""[2]

5 Methodologies for Information Security Awareness Program

Presenting a clear security awareness message to all employees in the organization can be achieved by variety of methods but all of them are not very effective and sometimes do not meet the requirements of the organization. These methods if implemented together lead to a comprehensive security awareness program. The organization can also chose any one of them to address the most critical and vital issue in the business without implementing a full fledge security program. All of these methods have the same core message, the employee responsibility and his behavior towards organization's information asset's security. Having different media and techniques to convey this message will get audience attention. They will be more attentive to new occurrence than to the same communication type and method every time.

Here are some of the methods to convey security awareness message across the organization:

- Information Security awareness training
- Computer based information security awareness
- Awareness services and reminder tools

5.1 Information Security Awareness Training

This is very mature, experienced and most effective method to get users attention in a class room environment. It helps to explain the subject and its contents in an interactive way. The contents of the sessions could be different as per the audience profile. Usually security awareness audience can be categorized into the following categories.

[2] National Institute of Standards and Technology Special Publication 800-50, Building an Information Technology Security Awareness and Training Program

- Management

The management is the ultimate and most important sponsor of the awareness program. He has a very specific need to understand the goals of awareness program and the role security plays in achieving their business objectives.

The presentation to the management should focus on security threats which organization may encounter in the shorter or longer run. It should be clearly communicated to the management that without its support the organization and the employees will not be able to protect information assets. Below are some of the management mistakes which have to be highlighted in the presentation.

  - Ignore security problems
  - Fail to realize the value of their information reputations
  - Rely primarily on technology/products.
  - Fail to deal with the operational aspects of security
  - Fail to understand the relationship of information security to their business
  - Not providing training/ time to their staff.
  - Always think quick and visible return on investment while implementing solution

- End Users

End users usually are not responsible for overall protection of the information. They must secure the work environment and the information they are dealing with. End users are involved in day to day activities and use data to perform their jobs. This type of audience requires detailed understanding of the information security threats, damage by those threats and solutions to mitigate the damage. They should also be familiar with the policies and procedures which will help them to ensure performance and security.

The underline message that should be communicated to end users is, consult your information security department whenever something went wrong or when ever you have questions. Here are some of the mistakes of end users which should be highlighted in the presentation.

  - Violation of security policy
  - Opening unsolicited e-mail attachments
  - Installing software from unknown sources
  - Visiting suspicious web sites
  - Not reporting security incidents

- Victims of social engineering

- Technical Staff

  Mostly it is understood that technical people do not require security awareness as they are the ones who designed the system so why should they be called for basic awareness sessions? The purpose of security awareness session for technical people is explaining them how technology is helping out business and what is needed to protect business and technology.

  Awareness session for technical people should be centered on technology is not driving the business, it is the opposite. It is always the business that decides the need of technology.

As discussed earlier, security awareness program doesn't mean one-size fits for all but topics have to be customized according to profile of the audience.

5.2 Computer Based Information Security Awareness

Some of the companies make awareness program easy and accessible for users at all times. They design a computer application and install it on the company's network which is available all the time. By using this self learning approach employees can access at their leisure and then learn by themselves the topics which are of interest to them. Mainly computer applications cover two basic modules and compliant with company security policies. The first module is a self assessment using a survey form. This helps users to assess where they are lacking in understanding company security policies. It's a good technique for users to analyze their strengths, weaknesses and compliance with company's awareness program. The second module is usually on the education of security issues, this helps users to learn and educate themselves the company security policies and procedures. Following are some of the topics which education module should cover:

- Password Construction
- Internet Usage
- Telephone Fraud
- Physical Security
- E-mail Usage
- Viruses
- Desktop Security

- Social Engineering
- Identity theft

5.3 Awareness Services and Reminder Tools

As discussed many times before, the security awareness is a continuous process and it should be a part of employee's job description and work environment. Using reminder tools is one of the methods to keep employees updated on security awareness topics and remind them from time to time.

Below are some of the reminder tools available, organization can choose any or all of them as per its need and acceptance.

5.3.1 Multimedia presentation

Multimedia presentation on security awareness topics is a good and interactive tool. Employees can use it as a refresher on all the topics which they have already covered in awareness training. It is also a great help for remote users where to organize training is not cost effective.

5.3.2 Security booklet

Most of the people in the organization find it convenient to read hard copy of the subject instead of soft or electronic format. Booklet in this case is an effective tool to convey information security awareness message, organization's objective and user's responsibility in protecting information assets. The booklet can also contain information security related pictures, quotes and case studies to educate employees.

5.3.3 Security posters

It is widely said that pictures and images are more effective to convey one's message across different types of community. People are more prone and feel happy to see graphical representation. Organization can design posters on different security issues and themes and place them on public places like entry door, sports hall, dining hall, cafeteria, recreation room, and near the water coolers in the organization.

There are lot of web sites that offer free posters or free sample of them, you can simply download and print them out.[3]

[3]Vandenberg Security Awareness Council http://members.impulse.net/%7Esate/posters.html
The Information Warfare Site http://www.iwar.org.uk/comsec/resources/ia-awareness-posters/

5.3.4 Computer screen savers

Screen savers can be a good idea to promote security messages. Almost all of the employees in an organization use computers and have screen savers which appear while computer is idle. Screen savers can be developed by using security awareness messages, quotes or graphical representation of security related issues and installed on employee's computer.
A customizable free screen saver from Microsoft Corporation is available.[4]

5.3.5 Email shots

Most cost effective tool to remind users about security awareness is an email message. Email is widely used communication medium and most of the staff access email once in a day. Sending email periodically containing security awareness reminder is a good and effective tool.

5.3.6 Promotional items with security issues

Gift items and promotional tools like Pencils, Pens, Erasers, Notepads, Mouse pads, Key chains, Cups or mugs etc can be printed with security wordings, quotes and pictures and distributed among people. This is also one of the motivational tools to remind employees of security issues.

5.3.7 Security Newsletter

Many of the big organizations publish monthly or quarterly official newsletter. Add security related news and messages in that newsletter and give free copy to all employees could be an effective reminder. This newsletter can also be used as motivational tool by adding best employee of the month/quarter. Who won prize on taking care of security issues, or by participating actively in protecting the company's information assets.

U.S. Department of Commerce/Office of Security
http://www.wasc.noaa.gov/wrso/posters/Security_Awareness_Posters1.htm

[4] Microsoft Corporation,
http://www.microsoft.com/Downloads/details.aspx?displaylang=en&FamilyID=6015F85B-9A3A-4AEB-8E50-28005312398A

6 Implementation of Information Security Awareness Program

It is management's and employee's responsibility to protect the company's information and resources. Implementation of the awareness program is also one of the responsibilities of both at their levels. Everyone in the organization has an important role and should contribute in implementing information security awareness and information protection program.

6.1 Implementation of Awareness Program Management's Responsibility

Due diligence and due care is part of Management's job. They are legally responsible and held accountable for integrity and security of corporate data assets just as they are for other assets of the corporation. Management has the final responsibility of implementation of awareness program as they have big picture of corporate activities and functions.

Information security is part of due diligence and due care, management support for awareness program is a critical factor and one of the most important contributors. It is management's responsibility to oversee the need of awareness and start implementation at its earliest.

6.2 Implementation of Awareness Program Employee's Responsibility

No organization can run without its employees. These are users of the data assets which is the soul of the organization's success and growth. Employees must understand the value of the information assets available on their network, computers and desks and be an active part of its protection. It is part of their job responsibilities and legal duty.

"Organizations don't change – people change. And then people change organizations."[5]

Without involvement of employees at each level, a security program will not be implemented or enforced, and upper management will not be able to provide protection of its information assets.

6.3 Implementation Techniques

There are mainly two main techniques of information security awareness program, and its implementation can be done by using any one or both of the

[5]Melissa Guenther LLC, http://hosteddocs.ittoolbox.com/MG052004.pdf

techniques.

6.3.1 Formal Technique

This includes:

- Security awareness tutorials/Training courses
- Formal presentations of security policies
- Professional articles in newsletters

6.3.2 Informal Techniques

This includes:

- Brief newsletter articles
- Quick notes
- Screen savers
- Posters
- Physical reminders like mouse pads, pens

Formal techniques of security awareness program are more professional and direct towards the subject. Informal methods have their own importance as people pay more attention to pictures, artwork and physical things. To make security awareness program successful and dynamic use diagrams, pictures and symbols.

6.4 Delivering Security Awareness

Implementation can be delivered in-house based on experience, understanding and knowledge or outsourced to consultants who will bring their own industry experience. Both internal and external resources can be utilized to benefit a program. The ultimate goal of any security awareness program must be to change the behavior of the people in the organization.

Successful implementation of security awareness program depends upon effective communication and delivery of the message and the subject. Following are the main factors of success:

- Who is your audience?
- What is the message you are planning to convey?
- How this message will be communicated?
- How often this practice will be repeated?

To achieve this you need a strategy which might include a logo, slogan,

common look-and-feel and templates. This will not only enable you to deliver consistent and clear messages, but will also enable your audiences to develop an understanding of what to expect. In addition, your audiences will be able to provide more valuable feedback on the information that they receive.

6.5 Obstacles in Implementation

Implementation of security awareness is a troublesome task and might face many obstacles from the users and at time from the management as well. Implementation also depends upon the staff and consultants who are leading this implementation and are the center point of communication both for the management and employees of the organization.

Just to list down some of the obstacles that could affect successful implementation of security awareness program.

- No management support
- Interaction with users, difficult to change their behavior and attitude
- No user's involvement in designing the awareness program
- Too much information without prior knowledge of users
- Lack of dedicated resources to run the program
- On size fits for all approach
- Employee turn over, program could be discontinued in the middle as employee leave the company
- Hire and train new employees, sometimes it is difficult to conduct screen out test and involve new employees in the awareness program

6.6 Post-Implementation

As we have discussed in detail security awareness is a continuous process that could not be completed if necessary measures are not taken to evaluate its success. You must get feedback from the participants and then update the program based on the results.

Post implementation deals with measurement, monitoring, effectiveness and execution of the program. It also addresses revision in the contents and methodology based on the results obtained from feedback, surveys and benchmarking.

6.7 Evaluation of Awareness Program

Evaluation helps to measure the success of awareness program. It identifies the weaknesses and strengths of the awareness program and is an essential part to

know the audience's behavior and topic of interest.

Periodic evaluation is not an easy task and requires lot of time and resources. Here are some of the techniques which can be used.

- Count the number and type of incidents before and after the program
- Survey by distributing questionnaire among audience
- Interview people individually and in a group
- Benchmark the program according to established standards
- Count the number of people participating in the awareness program and compare it with expected number of audience
- Audit the awareness program and the team who is responsible to design and implement the group

Evaluation of the awareness program is a must and gives following results.

- Statistics of awareness level before and after the awareness program.
- Statistics on awareness methods and topics interesting to the audience
- Helps to know whether objective and goals of program have been achieved or not
- Return on investment projection for the management

7 Motivational Factor in Implementing Awareness Program

Employee motivation is a vital part of successful and effective security awareness program. Regardless of the quality of awareness program and implementation methods, if employees are not keen to take part in the program, it would be a waste of time and resources. Employee should be motivated enough to look forward to being involved in the awareness program. They can accomplish this by protecting the company's information and by reporting any type of incident or deadly attempt by outsiders or insiders to access that information in a way that is not authorized.

The common question which all of the employee carry is: Why should we spend time on this type of programs which are not our responsibility and do not have direct impact on our job? Most of the people take security as a hurdle in their performance. They think the time they are spending on security issues could be utilized to enhance performance by doing more work which will be rewarded in monetary benefits.

An organization that is concerned about security and success of awareness

program must also include employee motivation strategies in the program and implement when and where needed. Along with many other types of motivational techniques following are very effective and have meaningful result:

- Appraisal and expectation of rewards for staff who actively participate and take interest in awareness program
- Fear of penalties and bad repute for those who don't take awareness program as a serious task
- Fear of personal loss
- Competitive environment among peers
- Annual information security week
- Nominate the best people who understand information security concerns and distribute prizes.
- Distribute gifts printed with information security related topics
- Review the performance of not only employees but audit top management and evaluate them on the same scale of appraisal or penalties
- Involve HR management in awareness program
- Add information security in job description, job description should include that the employee is expected to play and important role in the protection of the company assets. It should clearly have an impact on the employee performance bonus if the goals are not met. It should be clear that information security is not an optional component.

8 Conclusion

An information security awareness program is a vital need within any organization that wishes to ensure privacy, security, authenticity, effectiveness and availability of information assets. The success of awareness program depends upon management's consent and continuous support.

As discussed earlier, information security is a behavior and attitude rather than a technology issue. The only thing which can change is the behavior and thinking of the staff through awareness and education. People join organizations with their own beliefs, values, culture and principles. Information security awareness program facilitates those people to understand and take on the organization's culture, values and ethics.

"IT Security Awareness influences positive behavior and attitude changes of individuals, enhancing the overall security posture of organizations that rely on Information Technology to perform day-to-day operations."[6]

[6] GIAC Security Essentials Certification (GSEC) Practical Assignment Version 1.4b, IT Security Awareness Best Practices by: James Neidich

9 Reference:

1. National Institute of Standards and Technology, Building an Information Technology Security Awareness and Training Program, Special Publication 800-50
   URL: http://www.csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (February 7, 2005)

2. James Neidich, IT Security Awareness Best Practices, Oct 8, 2004
   URL: http://www.giac.org/practical/GSEC/James_Neidich_GSEC.pdf (February 7, 2005)

3. Robert Held, Security Awareness – are your users "clued in" or "clueless"? May 23, 2001
   URL: http://www.giac.org/practical/gsec/Robert_Held_GSEC.pdf (February 7, 2005)

4. Chris Garrett, Developing a Security-Awareness Culture –Improving Security Decision Making, July 23 2004
   URL: http://www.sans.org/rr/whitepapers/awareness/1526.php (February 7, 2005)

5. Chelsa Russell, Security Awareness – Implementing an Effective Strategy, October 25, 2002
   URL: http://www.sans.org/rr/whitepapers/awareness/418.php (February 7, 2005)

6. William Hubbard, Methods and Techniques of Implementing a Security Awareness Program, April 8, 2002
   URL: http://www.sans.org/rr/whitepapers/awareness/417.php (February 7, 2005)

7. Jeff Tarte, The Need for Information Security in Today's Economy, May 1, 2003
   URL: http://www.sans.org/rr/whitepapers/awareness/916.php (February 7, 2005)

8. Business Case for an Information Security Awareness Program, August 28, 2004
   URL:http://www.noticebored.com/NB_generic_business_case_for_infosec_awareness_program.pdf (February 7, 2005)

9. Donn B. Parker, Motivating the Workforce to Support Security Objectives A Long-Term View, October, 2002
URL: http://www.iwar.org.uk/comsec/resources/sa-tools/Motivation-for-Information-Security.pdf (February 7, 2005)

10. Melissa Guenther, Principles of Effective Security Awareness (SA) Communication
URL: http://www.iwar.org.uk/comsec/resources/sa-tools/Principles-of-Effective-Security-Awareness.pdf (February 7, 2005)

11. Melissa Guenther, Security Awareness Program
URL: http://www.iwar.org.uk/comsec/resources/sa-tools/Security-Awareness-Program.pdf (February 7, 2005)

12. Kelley Bogart and Melissa Guenther, Security Education and Awareness Communication, December 6, 2004
URL: http://www.iwar.org.uk/comsec/resources/sa-tools/Security-Education-and-Awareness-Communication.ppt (February 7, 2005)

Websites & online resources:

13. Awareness Training & Education Link, Computer Security Division National Institute of Standards and Technology, http://csrc.nist.gov/ATE/awareness.html (February 7, 2005)

14. Security Awareness Company
http://www.securityawareness.com (February 7, 2005)

15. Security Awareness Resource site
http://www.noticebored.com (February 7, 2005)

16. Melissa Guenther LLC
http://www.hosteddocs.ittoolbox.com/MG052004.pdf (February 7, 2005)

17. Security Screen Savers Page, Microsoft Corporation
http://www.microsoft.com/Downloads/details.aspx?displaylang=en&FamilyID=6015F85B-9A3A-4AEB-8E50-28005312398A (February 7, 2005)

18. Security Awareness Posters Page, Vandenberg Security Awareness Council
http://members.impulse.net/%7Esate/posters.html (February 7, 2005)

19. Security Awareness Posters Page, The Information Warfare Site http://www.iwar.org.uk/comsec/resources/ia-awareness-posters/ (February 7, 2005)

20. Security Awareness Posters Page, U.S. Department of Commerce/Office of Security http://www.wasc.noaa.gov/wrso/posters/Security_Awareness_Posters1.htm (February 7, 2005)