



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

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>

INFORMATION SECURITY AWARENESS POLICY

Andre Pretorius

10 April 2001

Introduction

In today's society, global companies use network security policies to ensure the implementation of their security model, in maintaining network security, protection of information loss, alteration, unavailability, and the safeguarding of the organisation's network from internal and external threats.

These implementations have often been neglected by users within an organisation, due to their misinterpretations, misunderstandings, lack in responsibilities and involvement towards information security in the organisation.

For this reason a security awareness policy was developed to ensure that all users involved in a computerised environment, to be on the lookout for any security risks that might occur. This awareness reduces the likelihood for threats from happening, and involves the user to take corrective steps if risks are being identified.

This document will explain the implementation of a security awareness policy and in what ways it is used to involve the user to be more alert towards security issues. The crucial role of management involvement will also be discussed, and how management decisions will affect the success of these security awareness actions.

Security Awareness Policy

The following points highlight the ways for every user to approach information security, and how to sharpen their awareness towards security concerns, by contributing to these issues.

Apply all password recommendations and features

Report any suspicious activity immediately

Never leave your workstation unattended

Take note of any security documentation received

Scan data and files regularly for viruses

Always attend all security meetings and courses

Never share user privileges

Do not exceed user rights

Alert your superior if your security identity have been revealed

Never repair security problems yourself

Share experiences and recommendations you might have

Apply all password recommendations and features

The use of appropriate passwords is of high importance for any computer system. All users should use appropriate passwords (at least 8 characters long, combination of characters, no words related to the user.) Passwords should be kept secret at all time, never shared with anyone, or stored on the workstation unless encrypted. All passwords should be changed on a regular basis.

Report any suspicious activity immediately

Suspicious system activities, files missing from the system, and unrecognised user ID's should immediately be reported to any superior or system administrator. Most threats towards the system usually occurs from inside activities.

Never leave your workstation unattended

All users should protect their workstation when leaving for lunch or a small break. Workstations are most vulnerable when left unattended and should be protected. Methods to protect workstations may include the use of a special "hot" button to enable the protective mode when out, or the use of a screen saver password.

Take note of any security documentation received

All document received regarding security issues should carefully be read. Documents

may provide important information regarding meetings, security courses or new warning about viruses or other threats. Notice boards contain important notes and should be checked on a regular basis.

Scan data and files regularly for viruses

All files and data kept on the workstation should regularly be scanned for viruses. Viruses come out all the time and all systems should have the latest virus updates, installed. No data downloaded from outside connections, like the Internet or received from unknown sources should be trusted and immediately checked for viruses.

Always attend all security meetings and courses

Meetings regarding security issues is vital to alert the user about important matters and always should be attended to. Courses should be integrated to extend the users knowledge about awareness and all new staff is obliged to attend the recommended security course.

Never share user privileges

User identities should never be shared with anyone, regardless the fact that he/she might be the users best friend, family member, staff member etc. Only the user himself may use his identity and privileges. Tokens, access cards, pin numbers or whatever security mechanism may not be shared between anyone and should immediately be reported if lost or stolen.

Do not exceed user rights

The user should never try to access a system where he/she has no user rights. Unauthorised system log-on's may mislead system personnel and distract them from real threats. Users should always arrange with their system administrator if they are in need of information, or require access to essential resources that is out of reach.

Alert your superior if your security identity and key have been revealed

The security manager or other security personnel should immediately be alerted whenever the users security identity or key, have been revealed. This might happen when the user accidentally revealed their password, or access card being lost or stolen

Never repair security problem yourself

Whenever it's a system failure, unauthorised access or data exploitation, users should restore changes by notifying the system personnel, instead of repairing the problem themselves.

Share experiences and recommendations you might have

Users should share problems and recommendations among their colleagues. Shared experiences, help users and management improve the awareness approach, and highlight the importance of these implementations in safeguarding the organisation.

The role of management in the security awareness implementation

Management should play a very distinctive role in the establishment of a well-defined awareness policy, by means of an organisational strategy approach.

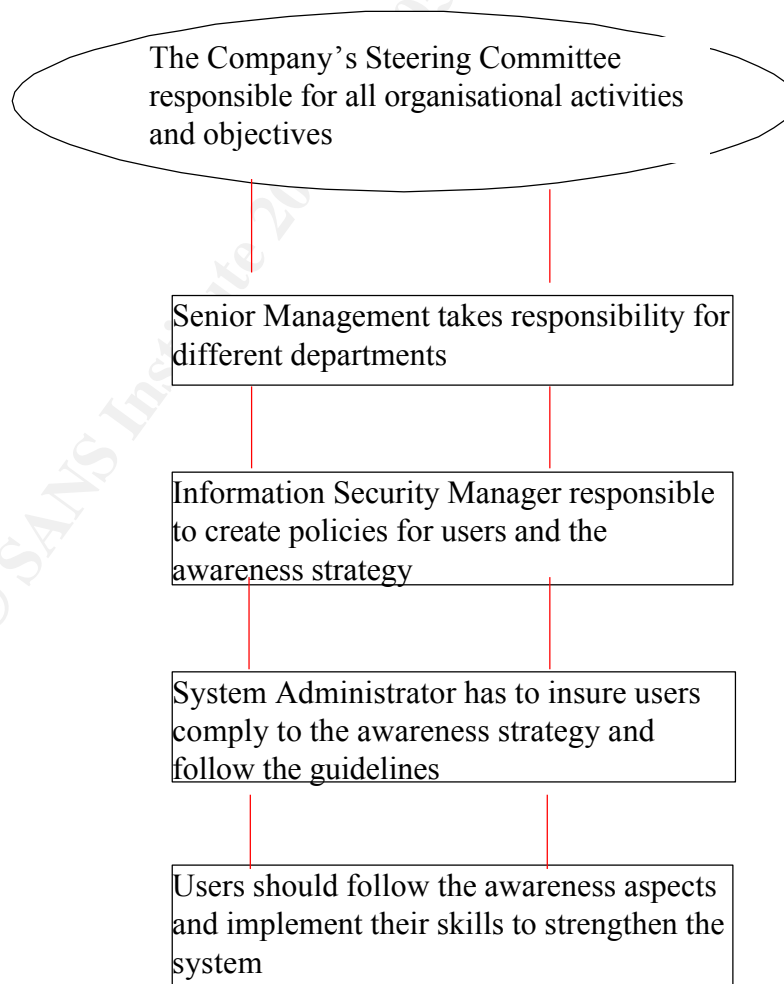


Fig 3.1 The Management's Implementation of Awareness

The organisational structure divides the awareness strategy from top management to lower levels to ensure changes are globally recognised.

Top management should acknowledge the need for the awareness approach, by means of the security concerns, and divide responsibility among senior management with a follow-up request at a given point of time.

Senior management should organise the responsibility in a more comparative way, and take corrective action if security measures have not been implemented. Their tasks consist in the development of an awareness policy and implementation strategy among users.

Security manager should be in charge of controlling and organising the implementation strategy developed by the senior management. All the awareness plans and policies should be reviewed, with given input if needed.

System administrators should be responsible for the operation and proper functioning of the system. They have to ensure that users comply with the security regulations, assist users with their responsibilities and monitor awareness strategies for maximum efficiency.




Users should strictly follow the recommendations and policies provided to them, and follow the regulations to ensure reliability and effectiveness. They should be alert for any possible threats and responsible to contribute towards system's safety.

Methods to improve personal skills and awareness knowledge

New staff training course on security awareness

All new personnel (including new employees and junior personnel), have to take part in the awareness course, this is essential to establish a healthy understanding of security concerns.

New staff will be inducted into the awareness strategy in the following way:

-  Receives an Information Resources Security Manual
-  Understands his/her responsibilities as a user of information resources
-  Can identify information security resources

- Understands the security awareness policies
- Can identify examples of sensitive and/or confidential data in his/her department
- Understands the repercussions of security violations

Discussing groups and previous problems

To keep up to date with security matters and findings, discussion groups and meetings should occur on a regular basis, to allow users to share their problems and solution's they discovered. These activities are important to enlighten concerns the organisation may experience, and how handle these in a proper way.

Some of the discussing issues may include the following:

- Users not following the security protocol correctly
- Viruses and Trojan's discovered
- Documentation not received
- Problems experienced, and solutions therefore
- New security programs
- Do's and don'ts on the system
- New courses to be attended

Monthly meetings

Monthly meeting are to be held in the discussions of security relates issues. The purpose of these meetings is strictly to encourage users to improve their awareness skills. The discussions involve the success of the security policies, problems or difficulties they experienced and solutions.

The success of various awareness implementations like messages, training courses, external testing and how it affects the system should be included in the discussion, with ways to be more effective in assessing risks and to add improvements.

Methods involving awareness of inside difficulties and system usage

External groups investigate strengths and weaknesses

The system should always be kept free from internal errors. Users may oversee their own faults and possible threats that might endanger the system. To ensure that most security problems have been addressed, and to avoid a subjective approach to the system, it is

important to use external specialist.

External specialists and consultants should do a thorough investigation on the environment and identify systems failures with recommendations. These findings are important for internal users in the identification of vulnerabilities, to sharpen their security awareness.

Way's external groups improve awareness result in the following:

- ☛ Attack the system from the outside and retrieve confidential information
- ☛ Discover users identity's and passwords by a simple inside attack
- ☛ Gain access to unauthorised departments by poor user management

User adaptability to new system

Implementation of a new system may result in great effectiveness (better security methods and devices) for the organisation, or might have disastrous consequences (if the default security implementations is not optimised). Users might not be aware of the functionality and usage of the system, and this may influence the effectiveness of security.



A throughout discussion is needed to upgrade users skills. Users should be clearly informed about the functions of the system, by undergoing training courses to improve their adaptability to the changes, and to ensure they understand all security implementations of the system.

Methods implying physical and visual awareness

News letters and e-mail containing warnings and important news

Users should always be aware of important matters and decisions within the organisation, to be more alert users about serious security issues. Important security topics in e-mail's or weekly newsletters should regularly be reviewed for relevant information as the following.


- ☛ Virus warnings about active viruses on the system, or via e-mail
- ☛ Unsafe Internet sites that should be avoided
- ☛ Flaws in current software versions that should be upgraded

-  Software that should not be downloaded
-  Attacks that happened on the system


Visual awareness methods

Visual methods should be implemented to remind the users towards their security obligations and sharpen the awareness to be security concerned all the time. A variety of simple methods with healthy results could be used.

Methods to be activated in improving awareness include the following:

-  The use of a key holder with digital password (SecureID)

Key holders with a random generated digital password (every minute etc.). The key holder is synchronised with the company's passwords server and every password is unique. The user should always be in possession of the key holder and supply the password when needed to access the system. This method enforces the user to use a password.

-  Flyers, stationary and gifts

The use of flyers and banners results as a good strategy to improve awareness among users. Invitations such as a security awareness week and security seminars could be distributed via this technique. Stationary and gift with security phrases may be used to create a more positive attitude towards user involvement and awareness.

-  Workstation reminders

This is helpful when passwords need to be changed or for new implementations by the user. A workstation reminder like screen warnings, or dialogue boxes could be implemented to alert users about these changes.

Methods involving network awareness and outside connections

Reminders via network messages

Network messages via pop-up dialogues are an efficient way of reminding users about

their security responsibilities. These kinds of messages may reach a vast number of users instantly.

The security responsibilities send, should contain matters that may seek immediate attention and be used for warnings like system shutdown, network virus invasion, network drives not to be accessed or files not to be downloaded or installed

Internet awareness

A special focus about Internet usage should be implemented. All users (with special attention to new users), should be educated about the dangers of Internet applications, and be familiarised of what content might be malicious, with the necessary browser security settings in place.

Internet restrictions should be specified implicitly, in stipulating what user rights and privilege is acceptable. This strategy furthermore involve ways of notifying users to download and send information in the right manner, and how avoid misuse of internet privileges may leave the system vulnerable to outside attacks.

Conclusion

"In order to maximize an organization's investment in security, indeed for that investment to make any sense at all, it is vital that the level of awareness of security issues among all employees of the organization be maximized."

Stephen Cobb, CISSP

The result of a successful security policy lies in efficiency of user commitment towards organisational security, their close interaction in ensuring secure system functionality, and the implementation of a successful security strategy with management plan. If user involvement towards information security is of non-importance, the system's defence will fail.

References

- 1) VGS Security Awareness Program, Bruce Johnston, 1999
URL <http://home.att.net/~vgscs>
- 2) Making your security policies work in practice, C & A Systems Security Ltd, 1999

URL <http://www.pcorp.u-net.com>

3) SAFE™ Awareness Program, Spectria InfoSec Services, 1998

URL <http://www.infosec.spectria.com/products/safe.htm>

4) Security Awareness For Everyone, Security Awareness Inc, 2000

URL <http://www.securityawareness.com/intranet.htm>

5) Information Security Policies made easy – version 7, 1999

Charles Cresson Wood

© SANS Institute 2000 - 2005, Author retains full rights.