Global Information Assurance Certification Paper

Name: Lim Ching Ching
Version: GSEC Practical Assignment version 1.3 (amended Dec 12, 2001)

Developing and Implementing An Effective Information Security Awareness Programme

Abstract

The purpose of this paper is to assist companies in developing a comprehensive information security awareness programme (ISAP), with the critical communication element built into the programme. It covers not only IT systems, but information residing on other medium (e.g. paper documents).

Management support is crucial to the success of this programme. Having firewalls do not imply that the company is secure; and the human element is the focus of such a programme.

Introduction

Security incidents are on the rise in many companies and it can happen to any organization – government or commercial (even companies providing security services). We read about security incidents regularly in the newspapers -- viruses causing major disruptions to large organizations, web sites being defaced or hacked, the use of computer systems to carry out fraudulent transactions, and so on.

> "The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls. Theft of trade secrets takes place despite the presence of encryption. Net abuse flourishes despite corporate edicts against it. Organizations that want to survive in the coming years need to develop *a comprehensive approach to information security, embracing both the human and technical dimensions.*"
> - Patrice Rapalus, CSI Director, about the CSI & FBI Annual Computer Crime & Security Survey

Information security is necessary not solely because of the increase threats but also due to the pervasive use of IT in most organizations. To mitigate the information security risks, companies have invested in technologies like firewall, anti-virus software, access control tools, and network monitoring tools. However, technology is only one of three essential components in raising the level of security in any organization. Ultimately, it takes people and process to make technology work properly to achieve the security goals.

People is the component that we will be focusing on. This is by far the most challenging aspect of security that any organization has to face – to convince their users that information security is everyone's responsibility, not to be left only to the IT department. The users need to be

convinced that not only the company's interest is at stake; ultimately, the staff's well-being may be directly or indirectly affected.

Critical Success Factors

- Senior management support

  Support from senior management in the form of endorsement of the plan, approval of budget, and provision of supporting staff to run the programme are necessary ingredients for success. A governance structure for information security, comprising of senior management, to set the directions on information security for the organization including the oversight of the information security awareness programme is a clear indication to the rest of the staff about management's commitment. On top of these, senior management have the opportunity to participate and contribute to the programme as I will share later.

  The programme champion, preferably senior management, must be identified. Since this programme require much communications and selling to the staff, the champion can be a role jointly owned by both the Heads of Communications and IT Security. A support structure should be set up to run and maintain the programme. This structure can comprise communications and information security representatives from every business unit to propagate the message and customize security issues so that they are relevant to their business unit.

- Relevance to recipients

  People tend to drift off or lose interest when confronted with boring topics like the policy or security controls as they view these as subjects that make their life difficult. Make it relevant to them by stressing that
  - information security policy protects them and clear distinguishes between what they can or cannot do (use analogy of traffic rules protecting drivers/pedestrians);
  - security controls protect their personal information (salary information or medical records);
  - their bread and butter is looked after (i.e. their job and bonuses) since security breaches can have a devastating impact on the company's brand name and bottom line (remember the last act by a disgruntled staff in Omega Engineering that almost crippled the company's operations, caused it to lay off workers and knocked the company off its top position in its industry).

- Participation by all

  This programme must reach out to all staff as security is only as good as its weakest link. It only takes one careless or ignorant staff to break that link. When developing the programme, the approach and communication medium used must vary to pitch at different levels of staff (senior management versus department heads versus junior staff).

Components of an ISAP

An ISAP has to take on a multi-prong approach in order for it to be effective. Other than the essential security awareness training, the ISAP must be complemented by a multi-media communications plan to reinforce the training.

- Mandatory training course for all

  All staff, from the most junior staff to senior management, must attend information security awareness training. The training can be conducted internally or outsourced. Training done internally would be more effective as the trainers are equipped with the relevant examples that they can use to relate to their colleagues. Subsequently, web-based training can be used as a refresher or reinforcement of the traditional classroom training conducted.

  The course can be modularized so that it can be customized for the various audience types depending on the kind of environment that the staff is exposed to (e.g. a group who is given a desktop/notebook versus another group who is only given remote access or use of shared terminals).

  At the end of the training, staff are required to sign an attendance form which states they have undergone the training, know their roles and responsibilities, and aware of the consequences if they breach security. This would then be filed with their personal records. Hopefully, the company would not require this in future as proof that the staff was aware of the wrongdoings when the breach was committed.

  The 7 modules would cover the following areas:

  - *Security Threats & Defenses*

    This module should cover the possible types of internal/external breaches that can happen to any organization through use of real-life examples. The possible perpetrators can be anyone – hackers, vendors, developers, business partners, visitors or disgruntled staff. To defend against such threats, organizations will take on preventive, detective and recovery measures. Awareness training is incomplete without alerting staff to social engineering techniques used by hackers. It is the human's tendency to be helpful; however they should be careful about offering sensitive information (e.g. IP addresses, version of operating systems used, passwords) to strangers without authenticating them.

  - *Company's Information Security Policy*

    Within the first week in the organization, all new staff and vendors should be briefed about the policy, their roles and responsibilities. In addition, the consequences of unauthorized actions (such as disciplinary action, dismissal or legal actions taken) must be made clear to them. Subsequently all existing staff will go through this compulsory training course that will reiterate the above points.

Users must be reminded about the dos' and don'ts about the use of the company's IT resources (e.g. use of email, access to systems and Internet etc). This serves as a reminder for the organization that I worked for since all new staff are given a complete set of company's rules and regulations (including the dos' and don'ts about the use of IT resources) which they are allocated some time to read. They would then sign an acknowledgment form to indicate understanding and acceptance of the rules before they join the company.

The dos' and don'ts may cover the following:

- Usage for official company business only
- Access the Internet through approved gateways (i.e. use of modems prohibited unless permitted by the IT Security department)
- Company's email account not to be used in newsgroups' participation
- Code of conduct in the use of email including prohibitions on
  - Use of abusive or offensive language
  - Making defamatory statements
  - Making racial, religious or ethnic slurs
  - Circulating chain letters or spreading rumors

- *Desktop/notebook and viruses*

Staff are taught how to encrypt sensitive information on their desktops, and to logoff when they are away from their desktops (e.g. for Win2K machines, they should always press ctrl-alt-del buttons simultaneously and hit the 'enter' key). For users with remote access to the company's systems (via the Internet), logging off their account and clearing the cache are important steps that they should take so that unauthorized parties do not have to the information that they have accessed earlier. For users on cable modems connections at home, they should log off instead of having the connections continuously on to lower their risk of having their PC compromised by hackers.

With the onslaught of malicious codes every year, training would be incomplete without mention of viruses, trojans and hoaxes. Useful tips include:

- Do not open attachments from people you do not know.
- Keeping the anti-virus software updated.
- Virus warning should be forwarded to designated IT department for investigations/confirmation instead of forwarding email to everyone else they know.
- Legal consequences (e.g. fine and/or jail term) when one circulates rumors or statements intending to cause fear or alarm.
- Report strange messages to the helpdesk.

- *Account management: Userid and passwords*

Since password is the most basic level of information protection, staff must be informed about their accountability and responsibility. They are responsible for all actions performed by their account regardless of who actually performed the act. Also, warning

staff that their usage is logged and monitored will serve as a constant reminder to them, even after the training, that they should to use their access as authorized.

To help users, they should be taught good password habits:

- Use 8 alphanumeric characters (special characters are encouraged)
- Change password immediately upon receipt
- Change passwords regularly (e.g. every 90 days or more frequently for sensitive systems)
- Avoid use of same password in different systems
- Choose a good password:
  - Use the first character of each word in their favorite phrase (I buy lottery hoping 2 be a millionaire ! = Iblh2bam!) or
  - Combine two words with special characters (e.g. zip~%>lock)
- Passwords must not be shared. Under NO circumstances, users are allowed or required to disclose their passwords (not even to helpdesk).

- *Physical security*

Everyone (including visitors) on the company's premise are required to display an identification pass prominently. Staff should 'challenge' or question people when they see them without their identification. Too often, we see contractors coming by without any prior notice and starting work on the PCs (to upgrade the PC or re-partition the drives etc). Some staff may just be happy to get a new PC or have their PC problems fixed to be overly concerned about the authenticity of these contractors. Staff must be reminded that these third parties may be potential 'hackers', and it is their duty to perform checks such as verifying with the IT department.

Other common-sense tips include:

- Unwanted paper documents with sensitive information must be shredded, not to be used as recycled paper.
- Remember to retrieve originals from photocopiers/fax machines immediately
- Do not use memory mode on the photocopier/fax machines
- Pick up sensitive printout from the printer immediately.
- Check to make sure that someone do not 'piggy-back' and follow you into sensitive areas.

- *Use of authorized software*

Unauthorized software must not be used in the company to avoid breach of copyright, support and integrity issue (does the software carry a trojan?). If a staff requires any software for their work, they should bring it to the attention of the IT department for proper evaluation.

Some may think that it is acceptable to download and use freeware in the company. In many cases, freeware are restricted to only individual or personal use, not to be used in a company, for profit entity, government entity, or educational institutions.

- *Intrusion response and reporting*

  As staff are the 'eyes' of the company, they would need to be vigilant and not hesitate in reporting security breaches to their supervisor or the incident response team. At the same time, they should be cautioned about talking to external parties (e.g. the press or public forums, friends/relatives) about security loopholes in the company.

  One of the pointers which I found useful was the one given by the Computer Security Handbook on using stories and examples:

  > "Stories about real people and real consequences (people being praised, disciplined, or fired) are useful in presentations and courses…..The stories should also relate to situations and decision the audience will be facing."

  During the training, company incidents and lessons learnt will be shared with staff. One of my favorite incidents was one whereby a staff was sabotaged by another when the latter took advantage of the email account that was left logged on and a nasty message was sent out to everyone.

- Videos

  Videos can either be bought off-the-shelf or developed internally (with help from professional communications companies). These videos are used to complement the training course.

  There are quite a few companies that produce good quality security videos, such as those by the Commonwealth films (http://www.commonwealthfirms.com). Some government website (e.g. http://www.ida.gov.sg) also produced videos to promote awareness amongst end users.

  Another alternative would be to develop your own video. A hugely successful one that we had revolved around a possible crisis scenario where there is breach in security and the pricing on the website was slashed. Senior management starred in this video and emphasized on the importance of every individual staff in playing their part to uphold the security for the company. The cost of making the video is easily four times the price of a commercial video. However, the benefits greatly exceed the cost. They are:
  - Clear management support in the security programme as demonstrated by their participation in the video;
  - Usage of an appropriate security incident scenario which the staff can relate to; and
  - Retaining the rights to the video and therefore copies can be made and distributed internally without breaching any copyright laws and at minimal cost;

- Posters

Like videos, posters can be purchased from the Internet. There are interesting posters from Native Intelligence, Inc (http://www.nativeintelligence.com) that made effective use of analogies to make it easier for the learner to understand information security issues.

You can also develop the posters in-house with personalized security messages from senior management, together with their photographs. These personalized messages again symbolize management's support, and management can emphasize how their staff can help. This may seem like an election campaign (similar to some political campaigns in some countries), but it certainly will generate a lot of publicity for the information security awareness programme.

- Mascot

Mascots can be a useful tool for staff to associate with information security. One can choose
- a human character (e.g. person dressed in white/black to symbolize the right and wrong actions);
- an animal character (e.g. use of an owl to remind everyone to keep their 'eyes' open for security breaches);
- a mythical character (e.g. use of a dragon to guard the treasures of the company); or
- an object (e.g. use of hats to symbolize staff putting on their security hat on top of their day-to-day operational hat).

A 'identify the mascot' competition can be run to solicit creative ideas from the staff. At the same time, it would build a sense of ownership as well as create opportunities for staff to think about security.

One word of caution about the final choice of the mascot: culture and type of business are important factors in the selection criteria. Western dragons may symbolize doom and death in the Chinese culture, or the bear may signify the downside of the investment cycle if you are in the banking industry.

- Comics

Comic strips are much easier to digest as compared to the information security policy which may be several pages long. This is useful for staff, especially those who are not familiar or comfortable with IT, to be able to associate with the various scenarios played out in the comics. If a mascot is identified, the mascot can be the character consistently used throughout all the comics.

- Intranet website or Email

The policy, the dos and don'ts, the tips on securing information, internal/external articles on security issues (including recognition of staff who exercise good security habits) should be published in a central location where staff can have access to. Contact information should be

made available so that staff know who to contact if they need to report security breaches or to verify if their action would be deemed as a breach.

For events that warrant immediate action (e.g. an outbreak of a malicious virus), the email system would be a more appropriate medium of communications to the users to warn them of the attack. Such warnings should consistently come from only identified sources (e.g. IT Security unit); otherwise they should be treated as hoaxes which should only be forwarded to the appropriate department for investigations.

Launch of the awareness programme

The launch can be divided into 3 stages:

- Pre-launch activities

  Prior to the formal launch, there can be a series of activities to build up staff's curiosity about the awareness programme. Possible activities include:
  - Regular column in the company's newsletter on information security issues
  - Weekly tips on how staff can secure information (e.g. reminders on choice of good passwords and to log off). This can be done via the company's intranet website or logon banners.
  - Identify-the-mascot competition

- Formal launch by management

  Launch the programme with a bang, Senior management's participation is a must. A security exhibition can be set up for staff to view security videos, posters and comics developed as part of the awareness programme. The event can be recorded and posted on the intranet for staff who are not present at the event (e.g. overseas offices). The in-house communications team should be invited to cover the event for the next issue of the company's newsletter.

  Where possible, this launch can coincide with the official Computer Security Day on 30 November.

- Post-launch activities

  After the big bang, the most crucial part of the programme is this maintenance stage. All earlier effort will come to naught if the awareness programme is not sustained. Management should be updated on the progress regularly and the next year's plan and budget to be approved by them. A review of the programme should be done on an annual basis, together with a survey to determine effectiveness.

  Company-wide awareness training will commence after the launch. Security posters and comics should be issued to all departments on a regular basis (e.g. every quarter).

Measurements of Effectiveness

- Annual survey

  Prior to the start of the ISAP, a baseline measurement should be done to capture the initial level of awareness in the organization. Subsequently, annual surveys are conducted so as to measure the effectiveness of the programme as well as identify the areas for improvements.

- Security 'Phantoms'

  Make use of security phantoms (or inspection teams) to do spot checks of current and future situations. They can find out the number of people who did not log off, had their passwords written on paper or left confidential documents lying around.

  One of our 'phantoms' went around looking at email accounts that were left logged on when staff went out for lunch. He left his 'mark' by sending an email from these accounts back to the owners themselves. This is one effective lesson as such news spread very fast and soon everyone in that department either log-off or had their screen saver with password activated whenever they are away from their desktops.

Conclusion

An organization culture in which staff breathe and act in a security-conscious manner would not happen overnight. With proper planning, support and resources from senior management, you are well on your way to inculcate good security habits amongst your colleagues.

Citations of sources

1. Rudolph, K, CISSO, Computer Security Handbook, 4th Edition, Chapter 29.
   URL: http://nativeintelligence.com/awareness/chap29-1.asp (17 Mar 2002)

2. Native Intelligence, Inc
   URL: http://nativeintelligence.com (17 Mar 2002)

3. Infocomm Development Authority of Singapore
   URL: http://www.ida.gov.sg (17 Mar 2002)

4. Atterbury Foundation
   URL: http://www.atterbury.org/html/start.html (17 Mar 2002)

5. California Department of Corrections
   URL: http://www.cdc.state.ca.us/isu/awareness_1.htm (17 Mar 2002)

6. Commonwealth Films
URL: http://www.commonwealthfilms.com (17 Mar 2002)

7. Association for Computer Security Day
URL: http://www.geocities.com./a4csd (17 Mar 2002)

8. Indian Health Service
URL: http://www.ihs.gov/Cio/ITSecurity/Posters/index.cfm (17 Mar 2002)

9. Computer Security Resource Center
URL: http://csrc.nist.gov/ATE/awareness.html (17 Mar 2002)

10. Anti-Defamation League (Security Awareness for Community Institutions: A Handbook)
URL: http://www.adl.org/security/responsiblities.html (17 Mar 2002)

11. Schneier, Bruce. "Secrets and lies: Digital security in a network world". USA: John Wiley & Sons, Inc. 2000: 367-388.