Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Introduction and Education of Information Security Policies to Employees in My Organization

Like most multinational companies (MNCs) today, the organization that I work for has an Information Security Office (ISO) in each region, to meet the organization's need for safeguarding the brand name, information and corporate networks. The regional Information Security Office in Asia Pacific was setup in May 2000. One of the first responsibilities of the regional ISO was to introduce the Information Security Policies to all Asia Pacific staff and educate them on these policies.

Copyright SANS Institute
Author Retains Full Rights

AD

Name: Harbinder Kaur
Version Number: 1.2e

Introduction and education of Information Security Policies to employees in my organization.

Introduction

Like most multinational companies (MNCs) today, the organization that I work for has an Information Security Office (ISO) in each region, which oversees the following functions

- Development for Information Security Policy and Compliance
- Monitoring of Intrusion Detection, Investigation and Response
- Administration of System Access Control
- Security Assessment and development of technical papers
- Conducting Awareness, Education and Training

to meet the organization's need for safeguarding the brand name, information and corporate networks.

The regional Information Security Office in Asia Pacific was setup in May 2000. One of the first responsibilities of the regional ISO was to introduce the Information Security Policies to all Asia Pacific staff and educate them on these policies.

Ten Key Controls

The Asia Pacific office has a Business Conduct Policy document, which all staff sign when they join the company. However, the company realized that this document did not state the policies and procedures clearly with regards to information security, personnel security, compliance and business recovery planning to name a few.

As a result, a Ten Key Controls document was written which provides clear policies and procedures in the following areas.

1. Asset Classification
2. Business Recovery Planning
3. Compliance
4. Computer & Network Management
5. Information Security
6. Organization & Management
7. Personnel Security
8. Physical & Environmental Security
9. System Access
10. System Development & Maintenance

4 out of these 10 policies deal directly with Information Security. They are Asset Classification, Computer & Network Management, Information Security and System Access.

Why have Information Security Policies?

Information Security Policies are necessary to ensure that important data, business plans and other confidential information are protected from theft or unauthorized disclosure. If employees of any organization are not aware of these policies, they will not know what is expected of them when they handle such confidential information.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Every organization should have the physical aspect of security well taken care but if the staff are not educated on Information Security Policies, their lack of education, awareness and training would result in confidential information simply walking out the front door.

Therefore, it is very important that Information Security Policies be implemented and that all staff be educated and trained in these policies.

Information Security Awareness Program

A good Information Security Awareness Program highlights the importance of information security and introduces the Information Security Policies and Procedures in a simple yet effective way so that staff are able to understand the policies and are aware of the procedures.

As Ten Key Controls were only introduced to the organization last year, the regional Information Security Office had to educate all the existing staff on the 4 Information Security Policies, which are part of the Ten Key Controls. The training commenced in November 2000 for existing staff while new staff continue to be trained every month.

Listed below are some of the methods used to communicate the importance of Information Security Policies and Procedures to the staff in the Asia Pacific region.

- **Information Security Training**

  The Information Security Office conducted a number of sessions since November 2000 and still continues to conduct the hourly information security training sessions every month. The training introduces the Ten Key Controls and explains in detail the 4 Information Security Policies. The Information Security Policies cover areas such as the following

  - ***Information Classification, Handling and Disposal***

    All information must be labeled according to how sensitive it is and who is the target audience. Information must be labeled as "Secret", "Confidential", "Internal Use Only" or "Public". Documents that are labeled "Secret" or "Confidential" must be locked away at the end of the workday. Electronic information (Secret or Confidential) should be encrypted or password protected. When the information is no longer required, documents should be shredded while files should be electronically shredded.

  - ***System Access***

    No sharing of UserID and password is allowed and staff are made aware of their responsibility on safeguarding their user account and password. Staff are also provided with some useful Password Tips on how to select a good password.

  - ***Virus***

    All computers must have anti virus software installed and it is the responsibility of all staff to scan their computer regularly. All software and incoming files should be scanned and staff are advised to scan new data files and software before they are opened or executed. Staff are educated on the importance of scanning and how a virus can crash a hard drive and bring down the office network.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- ***Backup***
  Staff are advised that they are responsible for their own personal computer backup and they should backup at least once a week.

- ***Software Licenses***
  Software piracy is against the law and staff are advised not to install any software without a proper license.

- ***Internet Use***
  Staff are advised that Internet use is monitored. Staff should not visit inappropriate websites such as hacker sites, pornographic sites and gambling sites. No software or hacker tools should be downloaded as well.

- ***Email Use***
  Staff should not use the email system for the following reasons
  - Chain letters
  - Non company sponsored charitable solicitations
  - Political campaign materials
  - Religious work, harassment
  - And any other non-business use.

  Staff are allowed to use the email for personal use but within reason.

- ***Physical security of notebooks***
  All notebooks should be secured after business hours in a cabinet, in a docking station or with a cable lock.

- ***Internal Network Protection***
  All workstations should have a password protected screen saver to prevent unauthorized access into the network. For those using, Windows NT or 2000, they should lock their workstation. To prevent staff from downloading screen savers from the Internet, you can restrict the screen savers to the default ones which come with Windows NT or 2000.

  Alternatively, you can use the Visible Statement software offered by www.greenidea.com. The software uses animation and high quality graphics to illustrate 5 main areas of Information Security. Staff are reminded of the importance of information security in a fun and easy way whenever they see the screen saver.

  The software will show animated graphics on any one of these areas-
  - Leaving workstations unattended
  - Company Asset Protection
  - Bullet points emphasing important security policies
  - Password Protection, Software Piracy, and Shutting Down Properly
  - Challenging Strangers & Personal Property Awareness

- ***Release of Information to Third Parties***
  Confidential information should not be released to third parties unless there is a need to know and a Non Disclosure Agreement has been signed. It is the responsibility of all staff to safeguard the company's information.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The importance of Information Security and its protection is reinforced to the staff with the video – "UnderWraps – Information Security" from Commonwealth Films. Video is a very good tool for information security training. Commonwealth Films, www.commonwealthfilms.com has a good selection of information security videos on areas such as computer security, information protection, email and Internet abuse.

The videos available in the Information and Computer Security section at this web site are relevant in addressing the different kinds of scenarios where information can be compromised and stolen. A novel way of getting the staff to view these videos is to have a screening during lunchtime and provide some light lunch. A different video could be screened very two months or so.

A list of the videos could be listed on the internal website so that staff can borrow the videos and watch them at their convenience.

- **Computer Security Day**

  The Information Security Office (ISO) held a Computer Security Day where staff were introduced to how the ISO conducts Intrusion Detection and Monitoring. A password-cracking contest was held where staff were told to key in a good and difficult password. The purpose of the password-cracking contest was to highlight to users how easy it was to crack a password.

  This contest helped to show the staff the importance of a good password and why they were made to change their password every month.

  Computer Security Day will be held very year to help reinforce the message that it is everyone's responsibility to safeguard the company's information and data systems. Each year a different area of information security will be highlighted.

- **Information Security Website**

  An Information Security website was also setup on the local Intranet which provides staff with FAQs, ISO Forms, contact information, links to security websites and procedure for security assessment. ISO felt that a website was necessary so that staff would be able to get the information they require at one place quickly.

- **Information Security Newsletter**

  Another way to reach out to staff is through a newsletter, which ISO publishes on a quarterly basis. The newsletter is published on the ISO website and previous editions of the newsletter are also archived on the website. The first newsletter was published in 1Q2001.

  The newsletter is a way for ISO to inform the staff on ISO recent events and coming events. A regular feature of the newsletter is a "What is …?" section where we introduced staff to areas such as What is a Virus?, What is WYSINAWYG(What you see is not always what you get)? and What is a Firewall? The newsletter has a regular Home Computing Corner where staff are provided with information security tips for their Home PC.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Welcome Letter

As part of new staff education and awareness, the ISO developed a welcome letter, which is sent to all new staff via the email. The welcome letter consists of two parts. Part 1 is sent to the user after their Domain ID and Exchange account is created. Therefore, the first email they will read when they logon to the network for the first time, will be the welcome letter from ISO.

Welcome letter Part 1

The first part of the letter welcomes the staff to the organization and provides them with useful information in the following areas-

- How and when to contact Desktop Support for hardware and software problems
- Where to find the Ten Key Controls
- How to apply for Internet Access
- Best Practices for Password, Voicemail, Physical Access, Viruses and etc.

Welcome letter Part 2

The second part of the welcome letter is sent about 2 weeks later and introduces the staff to more information, which they should know in order to comply with the security policies. The following items are included: -

- How to apply for Remote Access
- How to maintain accurate Contact Details
- Should not auto forward office emails to an external email account
- Details of the next Information Security Training

Regular Communication

Besides the training events and yearly Computer Security Day, regular communication via the email is another effective way of reminding staff of the importance of security policies.

Security Brochures & Magnet

A bi-fold Security brochure is given to all staff who attend the Information Security training. The brochure provides some Dos and Don’ts, password tips, how to secure a PC and Internet Best Practices. Included in the brochure is a Travel Tips insert which provides business travelers with tips on what they should do before they depart, en route and at their destination.

Apart from this, staff also receive a magnet, which has the following tips on it. This way, staff will remember the tips when they look at the magnet.

- Backup your data regularly
- Do not share your Logon ID and password
- Use a password protected screen saver
- Don’t write down your password on any paper
- Scan email attachments and diskettes for viruses
- Lock Confidential data after use
- Use the Internet appropriately
- Don’t use unlicensed software

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **Dos and Don'ts**
  A Dos and Don'ts checklist is given to all new staff when they join Visa. As it may be sometime before they attend the actual security training, the checklist would be a good and easy way for them to learn about what they should and should not do. The information in the checklist is listed below.

Don'ts

- ✗ Do not share your password with anyone including staff
- ✗ Do not write your password on any paper, whiteboard or post it pad
- ✗ Do not use easy to remember words as passwords e.g. Aug2001
- ✗ Do not use personal information or any word in any language spelled forwards or backwards in any dictionary
- ✗ Do not visit inappropriate web sites e.g. pornographic or hacker web sites
- ✗ Do not download unlawful or unlicensed software from the Internet
- ✗ Do not install unlicensed software onto your computer

Dos

- ✓ Do change your password regularly for every Visa system
- ✓ Do use a combination of letters, symbols and number for passwords
- ✓ Do use difficult passwords which are at least 6 characters long
- ✓ Do enable your Screen Saver Password or lock your workstation
- ✓ Do scan your computer regularly for viruses and any diskettes as well before you use them on your computer
- ✓ Do check that your virus software patches have been updated when you receive the regular update emails from Desktop Support
- ✓ Do backup your data at least once a week. It is your responsibility to do so.
- ✓ Do lock away all confidential documents, files and diskettes at the end of each work day

Other methods of information security awareness

Besides the methods listed above, which the ISO in my organization has implemented, there are still a lot of other ways as listed below to continue the education, training and awareness process.

- Banner page
  A banner page could show a different information security tip each time the staff logs on to the network.

- If there is a virus outbreak, staff need to be informed quickly so that they do not inevitably spread the virus to other people. Notices should be places on all front doors in bright colors to advise the staff of the actions they should take. Different color schemes can be used to indicate the severity of the problem.

Measurement of the effectiveness of these training and awareness program

There should be a way to measure the effectiveness of the initiatives, which have been undertaken to spread the message of information security. Listed below are some methods, which can be implemented to measure the effectiveness of the information security program.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- **Web based training program**
  A web based training program of the Ten Key Controls has been developed which all staff have to complete and score above 90% in order to pass the test. This program has not been launched in the Asia Pacific region of my organization yet but will be implemented shortly. A high score by most of the staff would indicate that the training methods used have been effective.

  The program introduces the Ten Key Controls in a fun and graphical way. At the end of the program, there is a quiz, which tests your knowledge of the Controls. A pass over 90% would indicate that staff are aware of the Key Controls and what is expected of them.

- **Security self-assessment survey**
  A survey should be conducted once a year to ensure that all staff are following the information security procedures correctly. The survey would indicate whether more training should be conducted if majority of the staff are not acutely aware of information security policies and procedures.

Conclusion

Through a comprehensive training program, the Information Security Office has successfully educated and trained existing staff and continues to train new staff throughout the Asia Pacific region.

In order to keep the staff interested in the Information Security Policies, ISO has to continue to think of new and innovative ways to reinforce the importance of information security to all staff in the organization.

References

1. Commonwealth Films Inc. – www.commonwealthfilms.com/infosec.htm
2. Easyi -Information security training and awareness solutions -. – www.easyi.net//introduction/itcompliance.htm
3. Security Policies and Procedures – www.zylt.com
4. Interactive Screensaver – www.greenidea.com
5. Ten Key Controls document – internal company document.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**