ROLE OF INFORMATION SECURITY IN NEW EDUCATION POLICY AND GOALS

Dr A.Srisaila[1] and T. Srinivasa Ravi Kiran[2]

[1]Assistant Professor,VR Siddhartha Engineering College, Vijayawada, Andhra Pradesh, India, PIN:520007, Department of Information Technology.

[2]Lecturer, P.B.Siddhartha College of Arts & Science, Vijayawada, Andhra Pradesh, India, PIN:520007, Department of Computer Science.

ABSTRACT:

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 staffs are able to understand the policies and are aware of the procedures. The goals of an information security program are to ensure the confidentiality, integrity, and availability of information and organizational resources. Computer & network security in higher education reflect the philosophies, attitudes, or values of an organization related to a specific issue. This paper describes the importance of policy development for information security and different ways within a college or university setting to get the desired results.

Key Words: Education, ICT, Information Security, Networks

1. INTRODUCTION

1.1 What Is Information Security?

Information security refers to the mechanisms that protect data. Often those less familiar with information security consider it a mere technical control implemented into IT systems. In reality, however, information security is more than a mere technical control and must be understood as the study and practice of protecting data in all its forms (e.g., whether stored in an IT system or reduced to paper or another physical medium). It includes protecting data from all types of threats, whether those threats are perpetrated by malicious outsiders or individuals with legitimate accesses to IT systems and data. The practice of protecting data includes three distinct information security concepts, outlined in the following paragraphs. Confidentiality means protecting data, in all its forms, from unauthorized access throughout its entire lifecycle (from data creation to data destruction). Unauthorized access includes access by individuals not affiliated with the underlying organization storing the data (e.g., criminals and hackers). It also includes access by individuals within an organization who purposefully exceed their scope of authority in accessing information (e.g., individuals looking up the records of celebrities or other targeted individuals when they have no professionally legitimate reason to do so).

[a] Confidentiality is the information security concept most often implicated when an organization experiences a data breach.[b] Integrity means ensuring that data within IT systems (or recorded or reproduced on physical media) are accurate. This means that IT system creators and managers implement controls within the system to ensure that users enter and process data correctly and that conflicting data elements are identified and resolved. Integrity also requires that only authorized users have the ability to change, move, or delete certain types of data files. When data have integrity, they are considered accurate and can be relied upon for decision making [c].

Availability means ensuring that data are available when needed and that IT systems are operating reliably. Stakeholders can ensure data availability in a number of ways, such as designing IT systems that are “redundant” (e.g., installed in such a way that a failure of one component will not cause an entire system to fail) and resistant to attacks, as well as ensuring that users back up data regularly.

Common intentional and malicious information security threats to IT systems and data include malware, spyware, keystroke loggers; backdoor access to IT systems; phishing and targeted scams designed to steal user credentials; intentional misuse by someone with legitimate access; and denial of service attacks intended to make data unavailable. In addi-tion to intentional and malicious threats, those who manage IT systems and the data contained in them must protect them from unexpected or accidental events: natural disasters, power outages, and lost or misplaced IT resources (e.g., a lost thumb drive containing sensitive data). They also must protect data and related systems from the unintentional actions of legitimate users, such as the accidental deletion of important data, accidentally posting sensitive data to a public-facing resource (e.g., a web page), or sending it to the wrong person (e.g., via email).

2. RELATED WORK

Academic institutions face a barrage of information security incidents such as data theft, malicious software infections, hacks into their computer Networks, and infiltration of other entities via their networks.

Adverse impacts of these incidents include compromised private data and intellectual property, substantial financial losses, and potential threats to critical infrastructure, public safety, and national security. Despite these issues, little research has been conducted at the policy, practice, or theoretical levels, and few policies and cost-effective controls have been developed [1].

3. PROPOSED WORK

3.1 Information Security Training to Staff

The information security training 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 User ID and password is allowed and staff is made aware of their responsibility on safeguarding their user account and password. Staff is 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 is advised to scan new data files and software before they are opened or executed. Staff is educated on the importance of scanning and how a virus can crash a hard drive and bring down the office network.

Backup

Staff is 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 is advised not to install any software without a proper license.

Internet Use

Staff is 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 is 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 is 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. The importance of information security and its protection is reinforced to the staff with the video "Under Wraps 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, and 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.

3.2 Computer Security Day

The *information security office* (ISO) held a computer security day where staff was 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.

3.3 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.

3.4 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 is provided with information security tips for their Home PC.

3.4.1 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

3.5 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.

3.6 Security Brochures & Magnet

A bi-fold Security brochure is given to all staff who attends 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 receives 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

3.7 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.

3.7.1 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

3.7.2 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

3.8 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 out break, 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.

3.9 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.

3.10 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 is aware of the Key Controls and what is expected of them.

3.11 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.

4. 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.

5. REFERENCES

1. Steffani A.Burd, The Impact of Information Security in ademic Institutions on Public Safety and Security:Assessing the Impact and Developing Solutions for Policy and Practice
2. Commonwealth Films Inc.,www.commonwealthfilms.com/infosec.htm
3. Easyi-Information security training and awareness solutions, www.easyi.net//introduction/itcompliance.htm
4. Security Policies and Procedures, www.zylt.com
5. Interactive Screensaver, www.greenidea.com
6. Ten Key Controls document, Internal Company Document.