Creating a Security Awareness Program for the National Insurance Crime Bureau

By Karen Graczyk

Master of Science in Information Security

Lewis University

August 23, 2007

Table of Contents

Introduction

Often times protecting an organization's information assets are thought to be the sole responsibility of the Information Technology (IT) Department and many assume that it is accomplished using sophisticated technology. While the layered implementation of security technology is critical; it will not protect an organization against a social engineer [1]. IT professionals may debate about what is the best technology or implementation of it, but almost all will agree that the human element can defeat any such technology. An organization can minimize the vulnerability inherent in its employees through security awareness training [2].

The National Insurance Crime Bureau (NICB) is a not-for-profit organization that partners with insurers and law enforcement agencies to assist in the identification, detection and prosecution of insurance criminals. Through its investigations and partnerships, the NICB has access to various data sources and securing those information assets is critical to the success of the organization.

NICB has spent the last several years implementing various security technologies in an effort to properly secure NICB data and systems. Realizing that the organization could not stop at technology, the CIO established a business objective to develop and implement an information security awareness program for all employees. The program should be ready for deployment by September, 2007, reach all employees, meet industry standards for security awareness, and be accomplished within the current IT budget. This program is paramount to ensuring that people understand NICB's IT and organizational policies, responsibilities, and how to properly use and protect the IT resources that have been entrusted to them as employees of NICB.

To accomplish the goal of creating a successful security awareness program, the program was divided into four major pillars; design, development, implementation, and monitoring and updating [3]. To help establish the design, a needs assessment was done to determine the overall security training needs and provide a vehicle for senior management buy in. During this phase, key elements such as program scope, responsibilities, audience, objectives, and methods were identified. The next phase, program development, focused on the creation of training material. Selecting the topics and presenting the material in a way that engages the audience is instrumental in the overall success of the program. Program implementation was accomplished using a centralized program model [3]. Implementation included web based training with student testing to measure comprehension of the training material. Lastly, the program would require regular monitoring and updating when needed to ensure continued success and compliance. Each of the sections mentioned were to be developed in conjunction with IT and business and operational unit staff. The result NICB is expecting is an enhanced data security program through security awareness.

Review of Literature

The book “The Art of Deception” by the famous hacker, Kevin Mitnick discusses the human element of information security. The book provides countless examples of how employees can be manipulated to reveal what is necessary for even a novice hacker to obtain unauthorized access [1]. In most cases, the employee has good intentions but is simply unaware of such a threat. There is the common saying that one is only as strong as its weakest link and many agree that an organization’s employees are often times its weakest link. Informing employees of the possible security threats helps strengthen that weak link.

There are many interesting articles and surveys regarding security awareness topics, particularly passwords, removable media and internet and email use. One example [4], a recent study in London surveyed IT professionals at a local expo regarding their passwords and password habits. Participants were asked to provide their passwords in exchange for a candy bar. Of those asked 22% of IT workers provided their passwords. Many participants who elected not to give out their passwords still provided enough information on the questionnaire to enable their password to be constructed. While these participants may have felt that it was anonymous because they did not write down their names, they were wearing convention required name badges complete with their name and company. The survey also revealed alarming password habits, such as using the same password for all accounts, willingness to provide their password to another, and admitting that they knew other peoples passwords [4]. While the survey did not actually attempt to use any of the passwords to determine if they were indeed provided the actual passwords, it does raise serious concerns. The underlying theme in all of these articles and surveys is that awareness and education help prevent these threats from materializing into a serious security breach.

What happens if you have a security breach? There are tons of horror stories out there that can scare not only the typical home user who makes purchases online, but major organizations. NICB has determined that a security breach could result in the following types of loss:

- Loss of data
- Compromise of data
- Financial loss
- Loss of productivity
- Repair costs
- Loss of reputation

The struggle for many organizations is that it can be difficult to sell a return on investment for such training, thus a hurdle to obtain funding for the program's development. Quality training programs demand time and resources. Typically in small or not-for-profit organizations, contractor or vendor help may not be an option and the creation and implementation of such a program falls to the IT department as explained in the article "Security awareness training for SMBs" [5]. The National Institute of

Standards and Technology' Building an Information Technology Security Awareness and Training Program is an excellent resource and a great starting point for anyone developing security awareness. In addition, there are many text books on the subject of information security which can help in the development of training material.

Most literature agrees that there are certain security awareness topics that are fundamental to basic information security. These topics are listed below [5]:

- Social engineering
- Email use
- Acceptable use
- Internet use
- Mobile devices
- Userid and password protection and use
- Incident response

In addition to the topics listed above, each organization should address any internal policies which relate to information security. For NICB this would include the data classification and handling policy which is critical to the protection of information assets.

Program Design

To design a successful program, NICB's business objectives, strategic plan and partnerships must be supported. Additionally, the structure of both the functional units within NICB and the network architecture play a role. Lastly, the culture at NICB was taken into consideration. The program was to be designed in a way that would provide NICB the most benefit. To do this, the employees must understand the importance and relevance of the program.

Mission

The NICB Security Awareness Program will educate users on NICB's information technology and organizational policies, responsibilities, and how to properly use and protect the information technology resources that have been entrusted to them as employees of NICB.

Needs Assessment

To help identify the organization's current security awareness, an assessment of employee's information security awareness was conducted [6]. A survey was developed and posted on the company intranet site. Employees were instructed to complete the survey anonymously and only identify their department. The survey was designed to help identify the current level of understanding regarding information security principals by the employees. Below are the survey questions, next to each answer is the percentage of employees that checked that answer listed in parentheses.

Have you ever received Information Security training?

□ No ***(81%)*** □ At a previous employer ***(10%)***

□ Yes, externally ***(9%)*** □ Yes, internally ***(0%)***

Do you have a good understanding of the Data Classification Matrix and Data Handling Policy?

□ Unaware of the policy ***(0%)*** □ Lack of understanding ***(13%)***

□ A basic understanding ***(80%)*** □ Good understanding ***(7%)***

Do you share your password?

□ Never ***(80%)*** □ Only when necessary ***(18%)***

□ Only with my boss ***(2%)*** □ Yes ***(0%)***

Do you practice a "clean desk policy"?

□ I'm not sure what that is ***(26%)*** □ Never ***(0%)***

□ Sometimes ***(19%)*** □ Always ***(55%)***

What level of understanding do you have of basic information security principals?

□ Poor understanding ***(9%)*** □ Basic understanding ***(56%)***

□ Good understanding ***(26%)*** □ I don't know ***(9%)***

Are you aware of what a social engineering threat is and how to defend against it?

□ Unaware ***(80%)*** □ Basic awareness ***(17%)***

□ Very aware ***(3%)***

Do you know what steps should be taken if you suspect an information security threat?

□ No ***(45%)*** □ Yes ***(55%)***

Do you have a general knowledge of computer viruses and worms?

□ No ***(3%)*** □ Somewhat knowledgeable ***(87%)***

□ Very knowledgeable ***(10%)***

Are you aware of any regulatory requirements that you're required to comply with?

□ No ***(19%)*** □ Basic awareness ***(55%)***

□ Very aware ***(26%)***

Are you familiar with the Standard Operating Procedures that address Acceptable Use Policies?

□ Unaware of the policy ***(0%)*** □ Lack of understanding ***(0%)***

□ Basic understanding ***(64%)*** □ Good understanding ***(36%)***

At the end of the survey, employees were asked if they had any information security issues in which they would like additional information. Email and internet scams along with removable media were requested.

Since senior level management support is instrumental in a successful program, IT staff meet with each department head to discuss the goal of the project [7]. A review of the data classification matrix and handling policy was completed and any updates, in which the department head was the data owner, were made. The survey results were discussed, including a summary of their department's results. This also provided an opportunity to discuss any information security issues that pertained to that department and review any partnership agreements that they may have and if they have any impact on NICB's information security practices.

In the end, the needs assessment survey results made a strong argument for moving forward with the security awareness program. It also indicated that social engineering and incident reporting were two areas that needed focus.

Program Audience

The program was designed as a basic security awareness course in which all full time, part time, and contract employees will be required to complete. Key positions within the IT, Finance and HR departments will be required to attend additional external security training and education programs specific to the duties they perform. This additional information security training will be handled outside of this program.

Training Methods

When considering different training methods, location of employees was a major concern. NICB has approximately 325 employees and a majority of those employees work out of their homes. It was determined that it would be cost prohibitive to provide training in a traditional classroom format.

Various vendors which provide Web-based training packages were considered. Most provided customization of training materials to fit your organizations brand, mission and operating procedures (references [8] and [9], were vendors which were considered).

Some of the advantages of this type of solution are listed below:

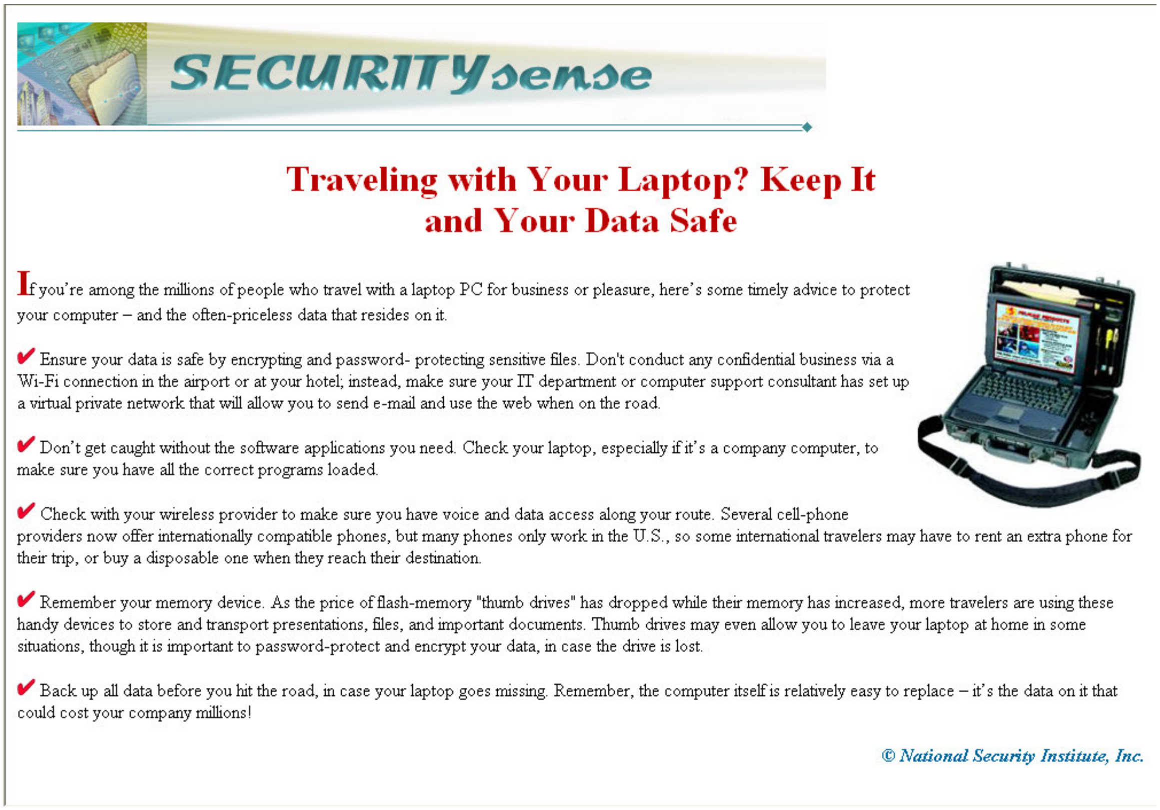
- Comprehensive training material
- Off site hosting and reporting
- Professional looking training material
- Customization
- Security awareness posters
- Certificates of completion
- Administration of users

- Regular updates that meet compliance requirements

The major disadvantage would be cost. Approximate cost to implement was $10,000.00 to $15,000.00. There were two major factors in costs; number of employees and amount of desired customization. Number of employees was based on total number trained, not total number employed. Therefore, if there is a high turnover rate, the number of employees could be significantly higher than the total number of positions. The vendors we looked into offered different pricing structures for customization, but the bottom line was the same. The more customization the organization requires of the training material, the more costly the implementation. With a slightly bigger investment up front the product could be purchased and implemented in house. This would decrease yearly costs, but increase other resources such as network and staff.

NICB also looked at a less expensive alternative called Securitysense. Secuirtysense would provide NICB over 200 information security articles and news stories a year (Figure 1) [10]. NICB could provide these articles to employees via email, intranet or posters. This service costs $1,000.00 for up to 5,000 employees a year. Some disadvantages of this solution would be the lack of customization and the inability to measure an employee's comprehension of the material [11].

NICB decided that an in house program developed by the IT staff, supplemented with a subscription to Securitysense would provide the most comprehensive training without an impact to the budget. The factors that contributed to NICB's decision were the number of employees, amount of customization desired and financial resources. The in house program would be a Web-based application delivered via NICB's intranet site.



Traveling with Your Laptop? Keep It and Your Data Safe

If you're among the millions of people who travel with a laptop PC for business or pleasure, here's some timely advice to protect your computer – and the often-priceless data that resides on it.

✔ Ensure your data is safe by encrypting and password- protecting sensitive files. Don't conduct any confidential business via a Wi-Fi connection in the airport or at your hotel; instead, make sure your IT department or computer support consultant has set up a virtual private network that will allow you to send e-mail and use the web when on the road.

✔ Don't get caught without the software applications you need. Check your laptop, especially if it's a company computer, to make sure you have all the correct programs loaded.

✔ Check with your wireless provider to make sure you have voice and data access along your route. Several cell-phone providers now offer internationally compatible phones, but many phones only work in the U.S., so some international travelers may have to rent an extra phone for their trip, or buy a disposable one when they reach their destination.

✔ Remember your memory device. As the price of flash-memory "thumb drives" has dropped while their memory has increased, more travelers are using these handy devices to store and transport presentations, files, and important documents. Thumb drives may even allow you to leave your laptop at home in some situations, though it is important to password-protect and encrypt your data, in case the drive is lost.

✔ Back up all data before you hit the road, in case your laptop goes missing. Remember, the computer itself is relatively easy to replace – it's the data on it that could cost your company millions!

© National Security Institute, Inc.

Figure 1: Example of Secuirtysense Article

Program Development

The needs assessment results reinforced the idea that the program should be developed in a way that would convey basic information security principals that the employees could relate to their positions as well as their everyday lives. The material should be interesting and relevant with comprehension of key security principals the goal.

Creation of Training Material

Four major training topics were selected; basic information security, identification and prevention of information security threats, incident reporting, and NICB Standard Operating Procedure (SOP's). From those four topics the outline below was created to help in the programming of the training material for the company intranet (references [3], [5], [12], and [13] helped provide topics).

1.0 Information Security

- 1.1 Introduction
  - 1.1.1 Definition
- 1.2 NICB's information assets
  - 1.2.1 Data Classification Matrix
  - 1.2.2 Information not classified
- 1.3 NICB's systems (provide a few system examples)
  - 1.3.1 Internet

    - 1.3.2 Email
    - 1.3.3 Databases
    - 1.3.4 Software applications
    - 1.3.5 Phone services
    - 1.3.6 Remote access services
  - 1.4 What is at stake
    - 1.4.1 NICB’s reputation
    - 1.4.2 Loss of productivity
    - 1.4.3 Loss or compromise of data
    - 1.4.4 Financial loss
      - 1.4.4.1 Repair costs
    - 1.4.5 Legislation compliance
  - 1.5 Securing information assets
    - 1.5.1 All employees are responsible
    - 1.5.2 Finding a balance between security and accessibility
    - 1.5.3 IT’s role in information security
- 2.0 Identification and prevention of information security threats
  - 2.1 Threats against your password
    - 2.1.1 How can a password be compromised
    - 2.1.2 What can happen if a password is compromised
    - 2.1.3 Better protection for passwords
    - 2.1.4 SOP 11.03 (Password Policies)
  - 2.2 Virus and worm threats

2.2.1 Viruses and worms defined

2.2.2 Potential destruction from viruses and worms

2.2.3 Preventing the spread of worms and viruses

2.2.3.1 SOP 11.01 and 11.09

2.2.3.2 Anti-virus software

2.3 Social engineering

2.3.1 Definition of social engineering

2.3.2 Examples of social engineering

2.3.3 Preventing social engineering

2.4 Mobile device threats

2.4.1 Examples of mobile devices

2.4.2 Theft of mobile devices

2.4.3 Shoulder Surfing

2.4.4 Wireless access points

2.4.5 USB devices

2.4.6 Removable media

2.4.7 Encryption

2.4.8 Deleting/wiping mobile devices

2.5 Insider threats

2.5.1 Potential motivation and loss

2.5.2 Possible Insider attacks

2.5.3 Preventing insider attack

3.0 Incident reporting

3.1 What should be reported

3.2 How should it be reported

3.3 What can be expected

4.0 NICB Standard Operating Procedures

4.1 Acceptable use policy

4.2 Email use policy

4.3 Internet use policy

4.4 Software and hardware acquisition policy

4.5 Userid and password policy

4.6 Software and hardware utilization policy

4.7 Anti Virus policy

4.8 Wireless communication policy

4.9 Physical access policy

4.10 Remote access policy

4.11 Ethics policy

Developing the Application

Development was divided into the following four sections; login, presentation of training material, measurement of comprehension (quizzes), and administration. Below is a brief explanation of each section.

Login

After clicking on the Security Awareness Training link on the NICB intranet, employees will be presented with a logon screen as seen in Figure 2. Instructions on the screen will direct employees to enter their assigned userid in the userid text box and their assigned password in the password text box and click submit. If the user entered their login information correctly, the home page of the Security Awareness Training application will display. If incorrect, the user would be instructed to attempt login again or contact the help desk for assistance.

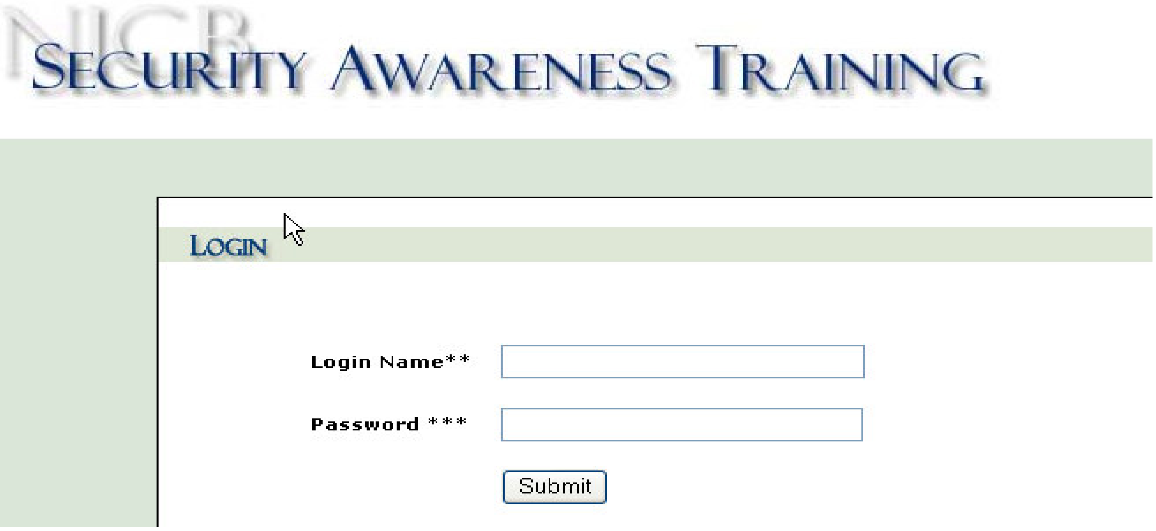
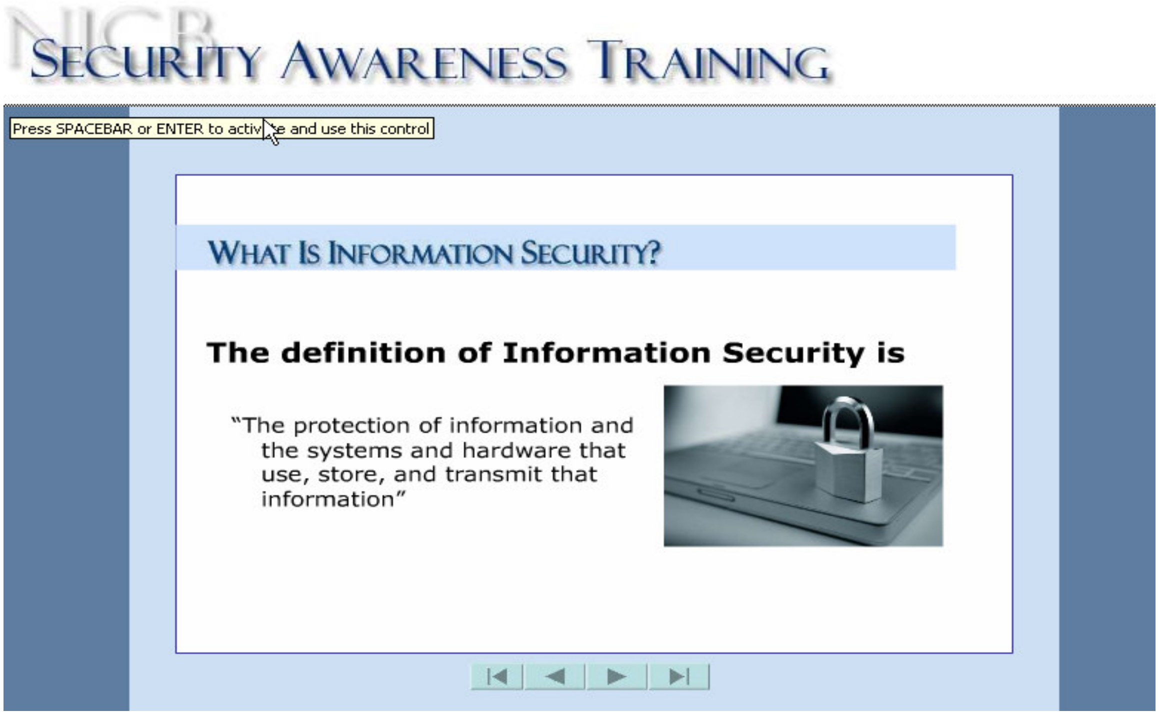


Figure 2: Print screen of application login

Presentation of Training Material

After CIO approval on the training material outline, the IT director created PowerPoint slides which were provided to the application developer responsible for the NICB intranet site. Using ASP, java script, and flash the application developer converted the slides so that the presentation of the training material was uniform in style with the overall NICB intranet theme. Less than twenty dollars was spent on art, which helped display the training information in a more appealing way. Additionally, the material will be presented at a pace controlled by the end users, through navigation buttons on the bottom of each slide as seen in Figures 3, 4, 5, and 6.



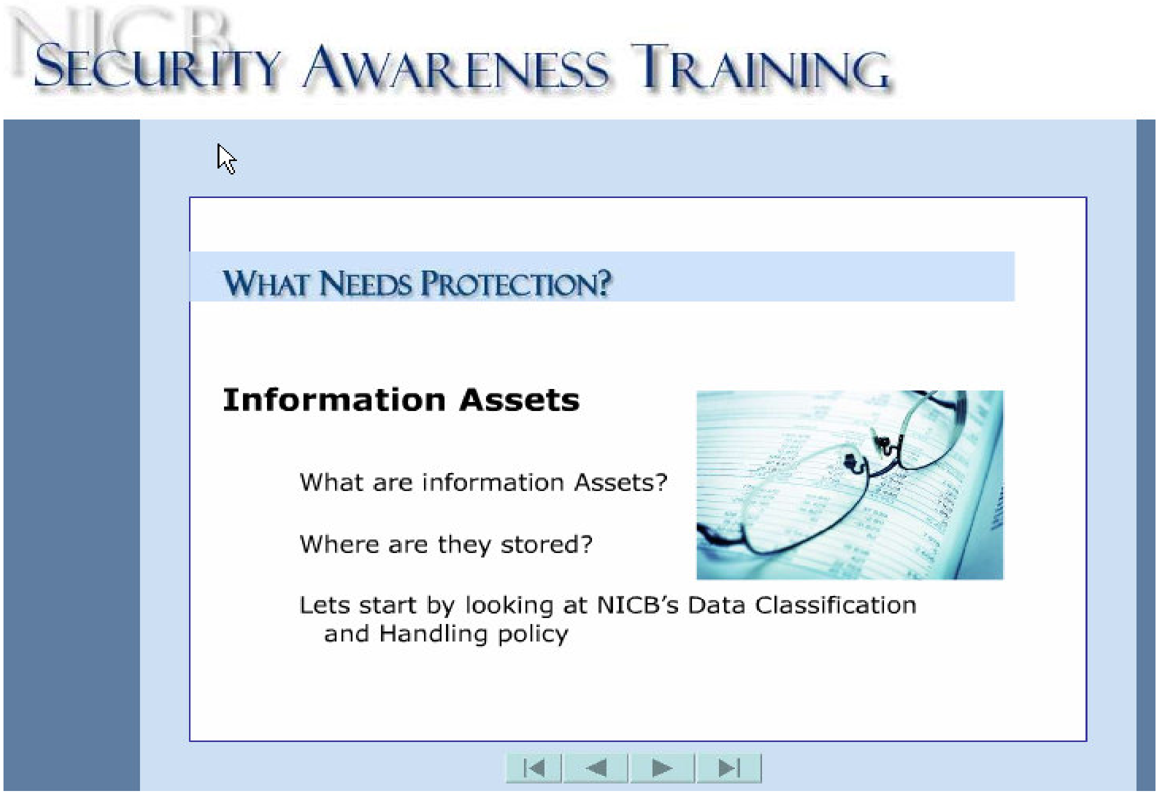
NICB Security Awareness Training

What Is Information Security?

The definition of Information Security is

"The protection of information and the systems and hardware that use, store, and transmit that information"

Figure 3: Print screen of a training slide



NICB Security Awareness Training

What Needs Protection?

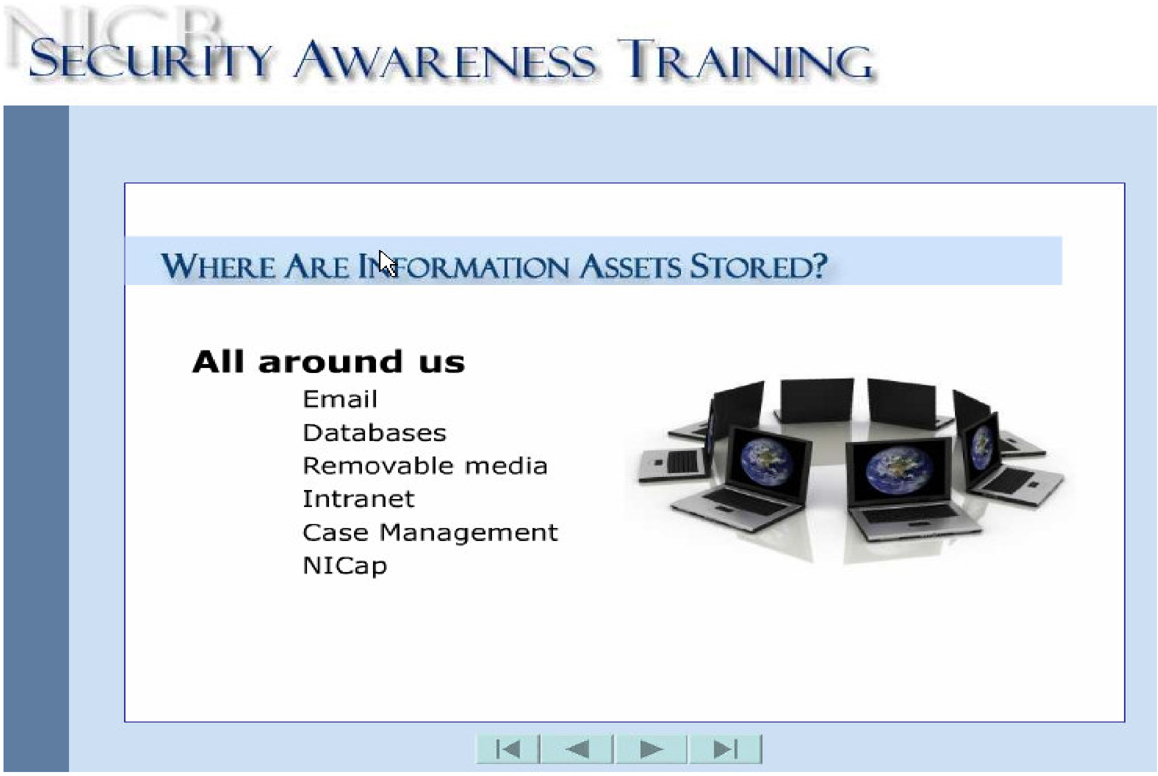
Information Assets

What are information Assets?

Where are they stored?

Lets start by looking at NICB's Data Classification and Handling policy

Figure 4: Print screen of a training slide



NICB

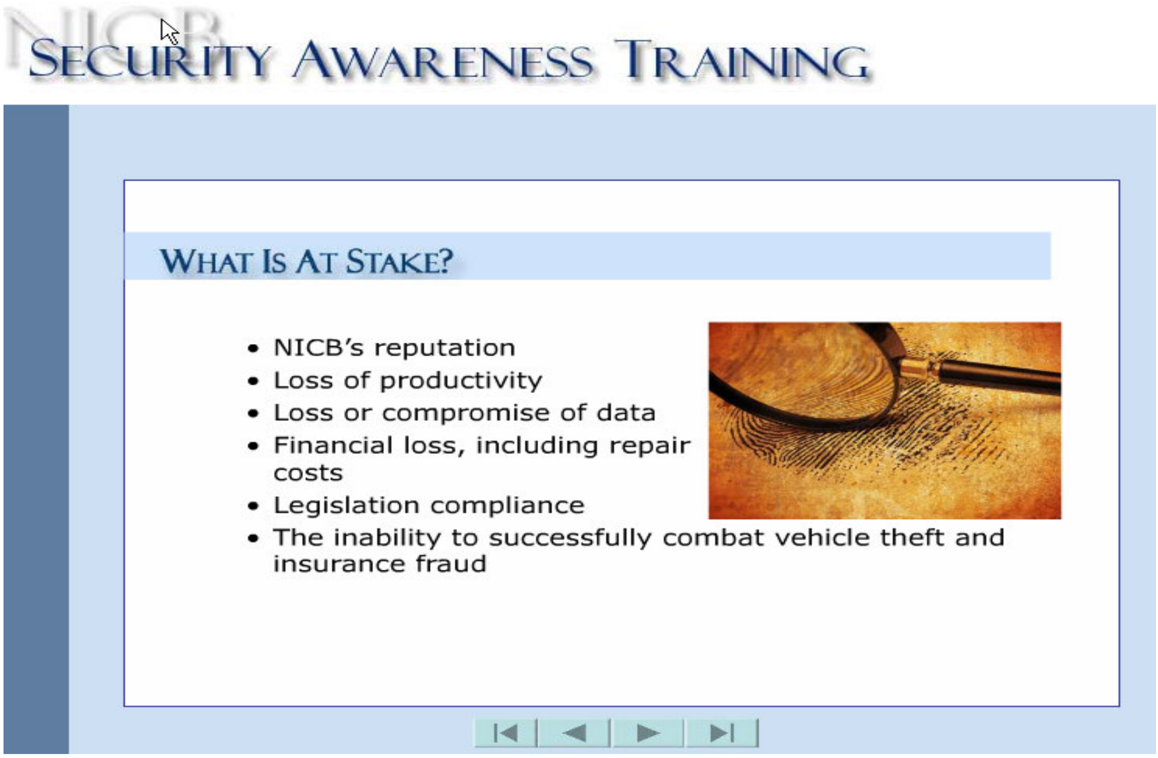
Security Awareness Training

Where Are Information Assets Stored?

All around us

Email
Databases
Removable media
Intranet
Case Management
NICap

Figure 5: Print screen of a training slide



NICB

Security Awareness Training

What Is At Stake?

- NICB's reputation
- Loss of productivity
- Loss or compromise of data
- Financial loss, including repair costs
- Legislation compliance
- The inability to successfully combat vehicle theft and insurance fraud

Figure 6: Print screen of a training slide

Measurement of Comprehension

Using java script, a total of four quizzes were developed and appear after each chapter of training material as seen in Figure 7. Immediately after submitting their quiz, the user will be presented with their answers and the correct answers. When the last quiz is submitted, an overall grade will be calculated and displayed. Users will not be allowed to retake a chapter quiz; however, users will have the option to retake the entire program if a final passing grade is not obtained. Users will have the option of exiting and resuming the program at a later time. The system will also store any quizzes that have been taken and users can easily determine which quizzes are remaining. Examples of the types of quiz questions participants will be expected to correctly answer are listed below:

Chapter 2 – Identification and Prevention of Information Security Threats

1. Which password would meet NICB complexity rules?

   A. Softball

   B. softball1

   C. S@ftball1

   D. All of the above

   The correct answer is C – S@ftball1. Password must contain characters from three of the following four categories:

   - English upper case characters (A..Z)

- English lower case characters (a..z)
- Base 10 digits (0..9)
- Nonalphanumeric (for example, !,$,#,%)

2. It is acceptable to allow someone else to use your login if you are going to be on vacation?

A. True

B. False

The correct answer is B - False - Individuals who have access to the NICB network **shall not** share their user ID and/or Password with **anyone** so as to prevent access to these systems utilizing their authority

3. Which program can be spread without human intervention?

A. Worms

B. Viruses

C. Email Attachments

D. All of the above

The correct answer is A – Worms. Worms can spread without any action by an end user.

4. If you receive an email you believe to be a virus, you should

A. Forward the email to your supervisor

B. Forward the email to the Technical Support Group

C. Delete the email

D. Contact the Technical Support Group

The correct answer is D – Contact the Technical Support Group. Never forward an email you suspect may have a virus. Always notify the Technical Support Group for further information and instruction.

5. If you are contacted by someone claiming to be from the NICB Technical Support group and they are asking for your login, you should do the following:

A. Provide them your login and advise your supervisor

B. Hang up on them

C. Inform them that you are not allowed to provide your password to anyone

D. Provide them the requested information, but only because they are Tech Support

The correct answer is C – Inform them that you are not allowed to provide your password to anyone. Social engineers will lie to trick you into providing them information that can be used to obtain unauthorized access.

6. Mobile devices increase your risks of the following:

A. Theft of equipment

B. Shoulder Surfing

C. Theft of information

D. All of the above

The correct answer is D – All of the above. It is important to be aware of your surroundings when you travel.

7. All of the following are techniques you can use to help prevent insider threats, except

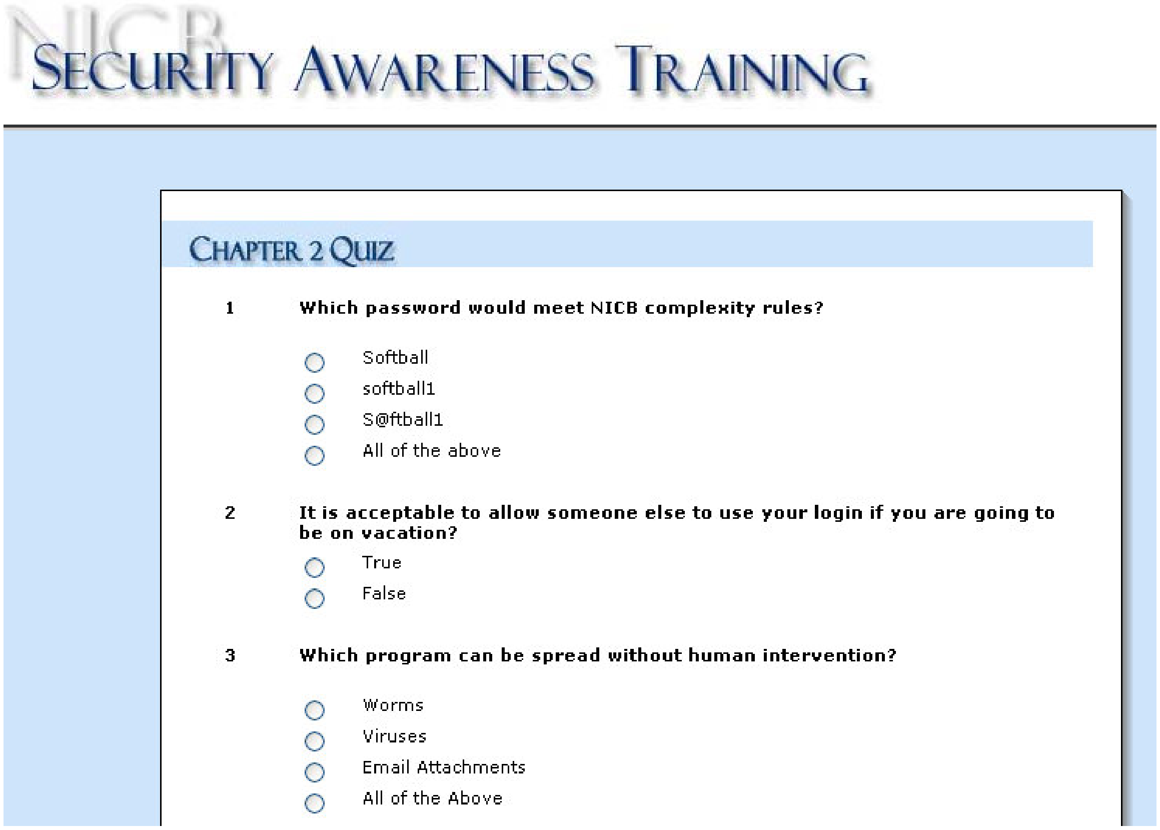
A. Keep your desk clean of confidential information

B. Do not send email attachments

C. When disposing of confidential information, shred it

D. Do not leave confidential information in shared workplaces

The correct answer is B – Do not send email attachments. Make sure to lock up all confidential information, even in shared workspaces.



NICB SECURITY AWARENESS TRAINING

CHAPTER 2 QUIZ

1 **Which password would meet NICB complexity rules?**

○ Softball
○ softball1
○ S@ftball1
○ All of the above

2 **It is acceptable to allow someone else to use your login if you are going to be on vacation?**

○ True
○ False

3 **Which program can be spread without human intervention?**

○ Worms
○ Viruses
○ Email Attachments
○ All of the Above

Figure 7: Print screen of Chapter 2 quiz

Administration Function

Management functionality was developed so that the program could be properly administered. The application will tie into the Human Resources database and therefore eliminate the need to separately manage users. As Human Resources adds, deletes or modifies the employee database it will automatically be reflected in the security awareness database. Additionally, an email address was created so that the test results could be emailed to the Human Resources department and viewed by the appropriate associate responsible for program compliance.

A report section was also created within the administration section and access provided to Human Resources, IT and department managers in an effort to help monitor employee participation. Several different reports were created, which are discussed in the Program Monitoring and Updating sections of this document.

Program Implementation

A good implementation is important to ensure a positive attitude towards the NICB Security Awareness Program. Therefore, the program needs to be communicated effectively to both management and employees [7]. The communication should include program goals, measurement of success and required time frames.

Program Communication Plan

The program will be introduced to the department heads by the CIO through an interoffice memo (Figure 8). The CIO will further discuss the program and answer questions regarding it at an upcoming department head meeting. This first step of the communication plan is instrumental because it is an opportunity to further obtain management buy in. The CIO hopes to clearly communicate the goals and importance of the program. Each department head will be advised to communicate the same positive message regarding the program to his/her employees [7].

Re: Upcoming Security Awareness Training

NICB is an organization which is information driven. Information drives investigations, analysis, forecasting, and prevention of vehicle theft and insurance fraud. Security of this information is critical to the success of NICB. The Information Technology (IT) department reviews and enhances the current security technologies on an ongoing basis.

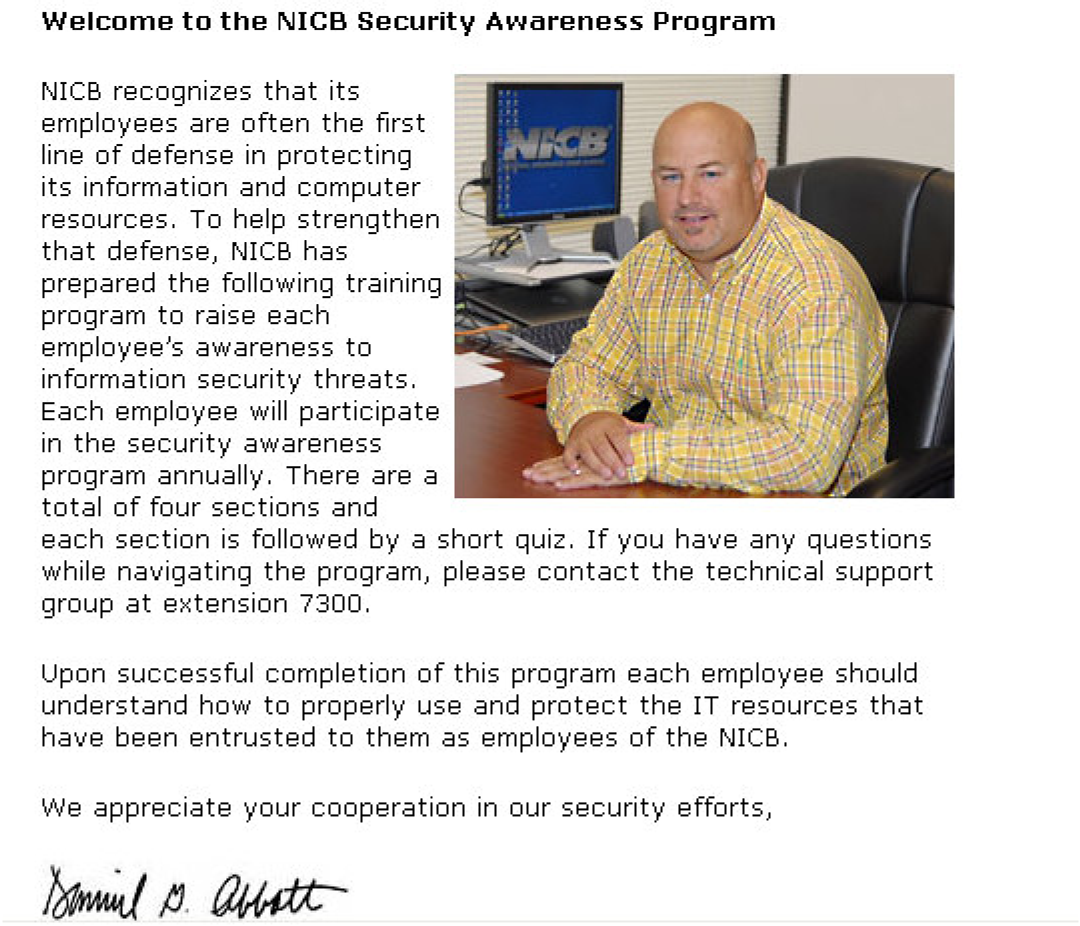
This is not enough. NICB employees are the first line of defense when it comes to securing the many information assets entrusted to NICB. It is this critical link in the NICB security chain that can make the difference.

To provide NICB employees the knowledge they need to properly identify and react to information security threats, IT has developed a security awareness program. This program will not only help employees protect NICB information assets, but their personal information assets as well. The program will deploy on September 4th, via the NICB intranet. Employees will receive an email from the CIO regarding a brief introduction to the program and the link to the program login page. Each employee will be expected to successfully complete the program within three months, successfully repeat the program annually, and make information security a priority. Please discuss this new upcoming program with your employees and stress the importance of its success.

Figure 8: Sample memo from CIO to Department Heads

The second step is to inform the employees. The management staff of each department will be asked to discuss the program. This discussion will be followed by a communication to the employees from the CIO. This communication will be in the form of an email and will be similar to the memo provided to department heads, which summarizes the program and its goals. The email from the CIO to the employees will be sent in early September and will provide the link to the security awareness program login page. A similar correspondence will be provided to new hires during their new employee orientation.

To further communicate the message to the employees, the following verbiage welcomes employees to the security awareness program on the intranet site (Figure 9).



Welcome to the NICB Security Awareness Program

NICB recognizes that its employees are often the first line of defense in protecting its information and computer resources. To help strengthen that defense, NICB has prepared the following training program to raise each employee's awareness to information security threats. Each employee will participate in the security awareness program annually. There are a total of four sections and each section is followed by a short quiz. If you have any questions while navigating the program, please contact the technical support group at extension 7300.

Upon successful completion of this program each employee should understand how to properly use and protect the IT resources that have been entrusted to them as employees of the NICB.

We appreciate your cooperation in our security efforts,

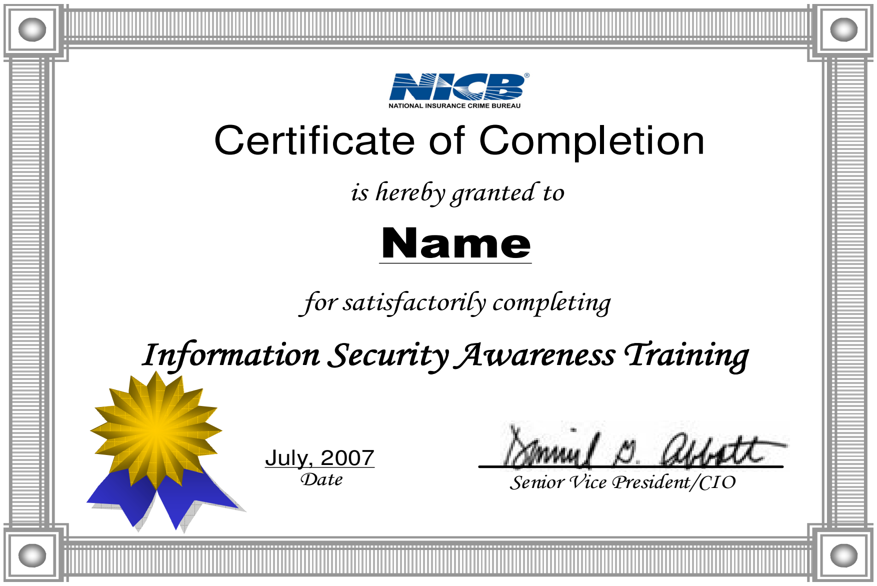
Daniel D. Abbott

Figure 9: Print screen of welcome screen

Success Criteria

If the goal of the program is to strengthen the defense of NICB's information resources, then each employee must have a basic understanding of information security principals upon completion of the program. To determine a level of understanding, a quiz will be administered after the employee completes each section of the program. The employee will be informed of the correct answer after each question. The employee will not be allowed to retake the section. Any employee who does not pass with a 92 percent or better will be instructed to re-take the entire program. Failure to successfully complete the program within 3 attempts will result in reduced access to system resources and require completion of an external security awareness training course.

Each employee that successfully completes the program will receive a Certificate of Completion, signed by the CIO as seen in Figure 10.



NICB
NATIONAL INSURANCE CRIME BUREAU

Certificate of Completion

is hereby granted to

Name

for satisfactorily completing

Information Security Awareness Training

July, 2007
Date

Daniel D. Abbott
Senior Vice President/CIO

Figure 10: Certificate of Completion example

The NICB CIO expects 100 percent compliance with the program. It is recognized that it is difficult to measure the success of the program as a whole; however the following objectives were identified.

- Limited number of information security incidents
- Proper identification of security threats by employees
- Proper reporting of security incidents by employees

To determine if the above goals have been meet the IT department will provide the following quarterly reports to the CIO.

Participation Report – This report will outline the number of employees which have taken the program, number of employees which successfully completed the program, and the number of employees which have not yet taken or successfully completed the program.

Information Security Incident Report – This report will detail any information security incidents identified during the quarter, including how and by whom they were identified.

Implementation Time

At the end of the development phase of the program six employees were selected to beta test the program. Beta testers were provided a brief overview of the application along with the link to the test server and a two week test period. Beta testers were asked to review course content, program flow, and usability. Feedback was provided to the development team and ranged from wording on training material to functionality changes. The overall feed back from the beta testing group was positive, and changes that provide site improvement have been made.

During the third week of August, a training meeting will be held for the technical support group so they can familiarize themselves with the program. The technical support group will field any questions employees may have while navigating the program. It is essential that this group provide the necessary assistance to employees.

NICB plans to launch the program in September, 2007. The program launch will be supplemented by Securitysense posters, which will be displayed on all employee bulletin boards and common areas. These posters will highlight an information security concept.

Each employee must successfully complete the program within the first 3 months of employment or implementation of the program. Each employee will receive an email annually on the anniversary of their successful completion date to retake the program. Again, employees must take and pass the program within 3 months of that date.

Program Monitoring and Updating

The monitoring and updating portion of the security awareness program is one of the most crucial parts of the program [3]. If NICB does not ensure compliance in the program and allows the program to become out of date, then NICB will fall short of the established goals. Therefore, steps have been taken to put in place a mechanism that will accomplish monitoring and updating of the program.

Program Monitoring

Management will have access to the management report page of the application. This section provides the capability to run reports based on department to help monitor participation in the program. The report will contain the following fields; name, anniversary date, completion date, most recent test score and number of attempts.

At NICB each area and department receives an annual inspection/audit. Starting in January 2008, security awareness will become part of the audit report. The Chief Inspector will review program compliance and will question interviewees regarding the program and information security concepts. Inspection interview questions will include but not be limited to the following:

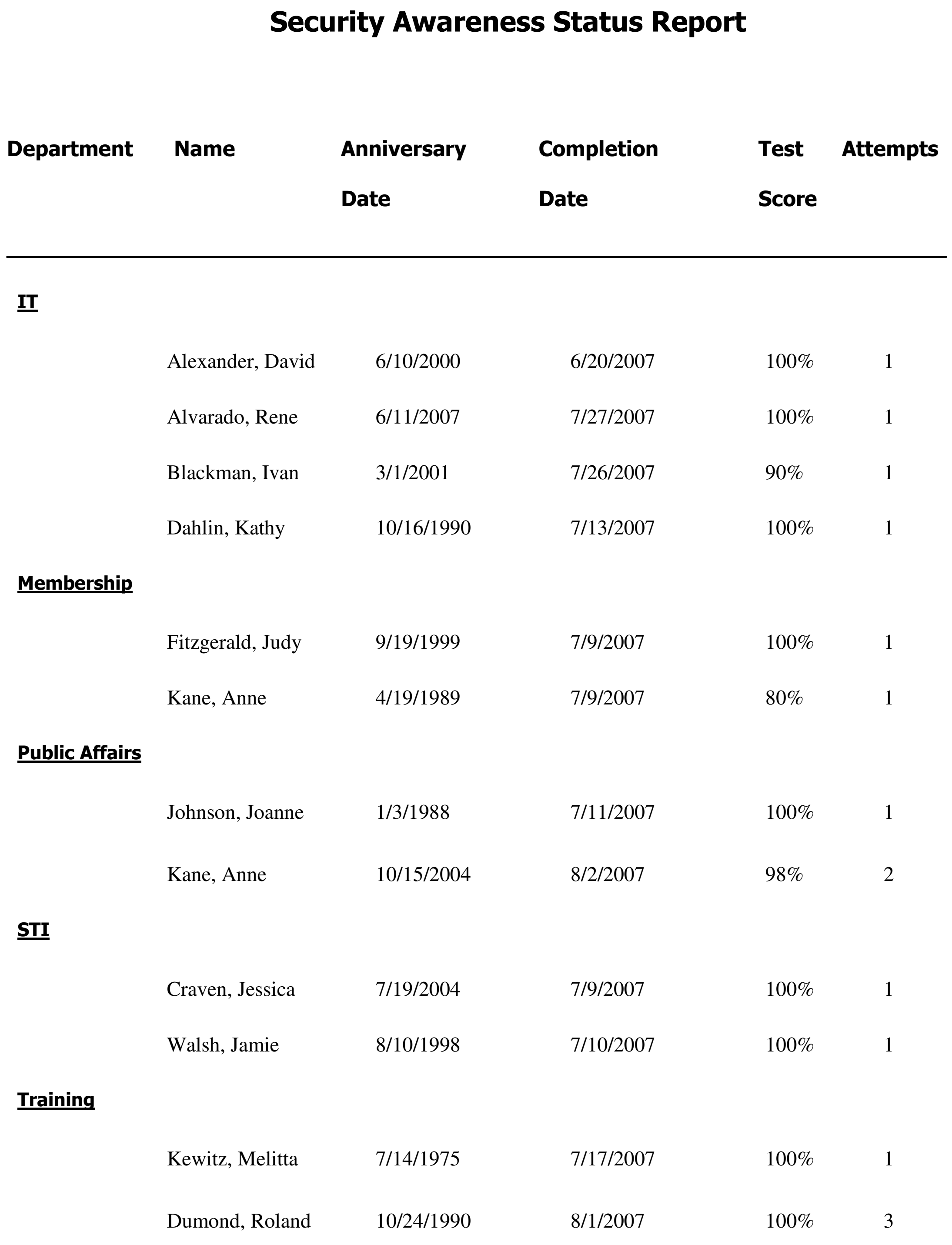
- Have you completed the NICB security awareness program?
- Do you have a solid understanding of the data classification and handling policy?

- Do you feel your access is properly aligned with your job duties?
- Have you identified a security threat in the last year?
- Are you aware of any information security issues or concerns?

The Chief Inspector will also perform a physical review of workspace to further ensure compliance. Some physical security concepts that the inspector will be looking for included but are not limited to the following:

- Employee access is controlled
- Visitor access is limited and monitored
- Employees practice a clean desk policy
- The handling of data is done in accordance with the data classification and handling policy
- Securitysense posters are displayed on employee bulletin boards and common areas

While Human Resources and the Chief Inspector will have the responsibility of ensuring employee compliance, each manager is expected to help facilitate program participation. Therefore, managers will have access to reports which provide a status of their employee's participation in the program (Figure 11). Mangers will be provided these reports on a quarterly basis or as requested.



Security Awareness Status Report

Department	Name	Anniversary Date	Completion Date	Test Score	Attempts
IT					
	Alexander, David	6/10/2000	6/20/2007	100%	1
	Alvarado, Rene	6/11/2007	7/27/2007	100%	1
	Blackman, Ivan	3/1/2001	7/26/2007	90%	1
	Dahlin, Kathy	10/16/1990	7/13/2007	100%	1
Membership					
	Fitzgerald, Judy	9/19/1999	7/9/2007	100%	1
	Kane, Anne	4/19/1989	7/9/2007	80%	1
Public Affairs					
	Johnson, Joanne	1/3/1988	7/11/2007	100%	1
	Kane, Anne	10/15/2004	8/2/2007	98%	2
STI					
	Craven, Jessica	7/19/2004	7/9/2007	100%	1
	Walsh, Jamie	8/10/1998	7/10/2007	100%	1
Training					
	Kewitz, Melitta	7/14/1975	7/17/2007	100%	1
	Dumond, Roland	10/24/1990	8/1/2007	100%	3

Figure 11: Sample management report

To help measure the success and/or areas of need, employees will be asked to once again complete the needs assessment which was utilized during the design phase of the program. The needs assessment survey will be conducted after the program has been in effect for one year. The results of the needs assessment will be compared to the original needs assessment to determine the impact of the program.

Program Updating

NICB realizes that a good security awareness program is one that is updated on a regular basis. Since employees will be required to complete the program annually, the training presentation material must be kept fresh. Examples used in the training presentation should be current as well as the artwork and therefore change at a minimum annually.

A security awareness team consisting of the IT Director, Application Developer, Network Administrator, IT Associates, HR Associate, and a Training Associate will be responsible for regular program updating. The security awareness program team recognizes that identifying updates to the program will be a challenging task. All changes in the organization or industry must be reviewed for an information security impact. Some of the areas to be discussed will include, but not be limited to changes in NICB policies, network structure, industry changes, application changes, staffing changes, course material, quiz questions, employee comprehension, employee opinion, and new/existing program goals.

In an effort to help identify areas which need updating, a series of reports will be available to the security awareness team. Each of the quarterly reports is described below:

<u>CIO Report</u> - Quarterly management reports will be provided to the CIO and the IT Director, which breakdown the different areas of the training program and provide a comprehension overview. This will help isolate sections or quiz questions which may need updating or additional training material.

<u>Program Questionnaire Summary Report</u> - Employee opinion of the program is important to NICB management. NICB believes in open communication between employees and management, and would like to encourage feedback. Employees will be asked to fill out and return a questionnaire upon completion of the program. The questionnaire will contain the following seven questions, thus keeping it short as to not burden the employees.

Security Awareness Program Survey

1. Do you feel you were provided an adequate amount of time to complete the program?

2. Was the program easy to navigate?

3. Did you have any issues with your login?

4. Do you feel the material was presented is a format that was easy to understand?

5. Did you find the program engaging?

6. Do you feel you have a basic understanding of the information security concepts presented?

7. Do you have any suggestion for improving the program?

Questionnaire results will be sent to a Training Associate who will evaluate and escalate any suggestions for program improvement. The Training Associate will also prepare a summary report for the program team to review on a quarterly basis. The summary report should help identify any portion of the program which needs improvement.

Technical Support Call Log Report - The NICB technical support group produces quarterly call reports which help identify software, hardware and training issues. The technical support group will provide the security awareness team a quarterly report which provides a summary of calls logged under the subject of security awareness program. This call report should further help identify any functionality issues of the website.

Inspection Report – The Chief Inspector will provide a review of the information security sections of any inspections conducted during the relevant quarter. This would include the responses to the interview questions as well as the physical security review.

In addition to the above mentioned reports, any NICB standard operating procedures (SOP) which has been updated during the quarter will be reviewed for impact. The CIO, IT director and network administrators are responsible for identifying changes in program goals, staffing changes, system changes, application changes, industry changes and world wide changes which may have an impact on the information security concepts presented.

Program Conclusion

Many programs like this are created in an effort to ensure compliance with auditors and the industry. However, a security awareness program can offer much more than that for an organization. It can result in well informed employees who take care to protect what information assets they have been entrusted.

One beta tester of the NICB security awareness program took the quizzes without going through the training material and obtained a score of only 30 percent. After reviewing the training material, the beta tester received a score of 100 percent. The beta tester commented to the security awareness team that learning about information security concepts was similar to teaching a child about the dangers of a stranger. Many people are new to the information world and they do not realize the potential dangers. The very thing at risk is the key to keeping it safe – information. This program is the avenue chosen to get that information to the employees and it is one of the most important steps to creating a secure computing environment at NICB.

The process of creating this program internally helped unite IT, low, middle and senior management in the drive towards better information security awareness. Everyone involved in the project came to realize just how easy it could be to have a security incident and developed a sense of urgency in getting the word out to the employees.

Future Direction

Future plans for the current website include adding voice to the training presentation material. This will enhance the training experience and increase compression of the material. The security awareness team has already begun developing script for the program slides and hopes to see this enhancement incorporated early 2008.

NICB believes that this program will prove to be valuable tool against information security threats. NICB also believes that it will serve as a foundation for future growth of the information security program. Ideally, each functional unit within NICB should have a supplemental module in the program which addresses information security specific to that unit or job function. Additionally, the expanded use of third party training material and courses could be utilized with an increase in budgeted funds.

References

[1] Mitnick, K.D. & W.L. Simon (2002). *The art of deception*. Indianapolis, Indiana: Wiley Publishing, Inc..

[2] Why train end users on security awareness. Retrieved July 17, 2007, from inspired eLearning Web site: http://www.inspiredelearning.com/sat/why_security_awareness.htm

[3] Technology Administration U.S. Department of Commerce. (2003). *Building an Information Technology Security Awareness and Training Program* (NIST Special Publication 800-50). Washington, DC: U.S. Government Printing Office.

[4] Cheung, H (2007,April 17). Workers give up passwords for chocolate and a smile. Retrieved June 10, 2007, from tgdaily Web site: http://www.tgdaily.com/index.php?option=com_content&task=view&id=31659&Itemid=118

[5] Dubin, J (2007, April 2). Security awareness training for SMBs. Retrieved June 10, 2007, from SearchSMB.com Web site: http://searchsmb.techtarget.com/tip/0,289483,sid44_gci1249866,00.html

[6] Volonino, L. & S.R. Robinison (2004). *Principles and practice of information security*. Upper Saddle River, New Jersey: Pearson Prentice Hall.

[7] Critical success factors for security awareness and training programs. Retrieved June 10, 2007, from Bits financial services roundtable Web site: http://www.bitsinfo.org/downloads/Publications%20Page/bitssecaware.pdf

[8] Security awareness. Retrieved February 8, 2007, from inspired eLearning Web site: http://www.inspiredelearning.com/sat/default.htm

[9] Online training. Retrieved March 4, 2007, from The security awareness company Web site: http://www.thesecurityawarenesscompany.com/products/online.php

[10] Traveling with Your Laptop? Keep It . Retrieved July 17, 2007, from SecuritySense Web site: http://nsi.org/SSWebSite/Samples/8feb07.html

[11] SecuritySense Solution. Retrieved April 8, 2007, from SecuritySense Web site: http://nsi.org/SSWebSite/Solution.html

[12] Egan, M. & T. Mather (2005). *The executive guide to information security*. Stoughton, Massachusetts: Symantec Press

[13] Whitman, M. E. & Mattord, H. J. (2003). *Principles of information security*. Canada: Thomson Learning, Inc.