

“You Are the Key to Security”: Establishing a Successful Security Awareness Program

Carrie McCoy
University of Missouri – Columbia
Information & Access Technology Services
615 Locust Street, Suite 200
Columbia, MO 65211
mccoymc@missouri.edu

Rebecca Thurmond Fowler
University of Missouri – Columbia
Information & Access Technology Services
615 Locust Street, Suite 200
Columbia, MO 65211
thurmondr@missouri.edu

ABSTRACT

Educating users on the importance of information security is vital to the mission of any IT organization. At the University of Missouri – Columbia (MU), we recognize that information security can no longer take a back seat to productivity and the two must go hand in hand.

We recently implemented a campus-wide information security awareness program to educate students, faculty and staff on this important topic. The program consists of in-person and web-based training, monthly topic-specific campaigns, presentations to specialized groups and guest speakers. The goal is to educate users on specific information security issues and to create overall awareness that will change the way people think and ultimately the way they act.

In this paper, we explain how we created and implemented our security awareness program and discuss the stumbling blocks we encountered along the way. We explore different audiences, methods of delivery and what content we believe is vital to a successful program. Finally, we discuss the importance of establishing a flexible program that can be adapted to meet current and future demands while still being relevant to our users.

Categories and Subject Descriptors

K.3.2 [Computer and Education] : Computer and Information Science Education

K.6.5 [Management of Computing and Information Systems] : Security and Protection

General Terms: Security, Human Factors, Management

Keywords: Security awareness, end-user education

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SIGUCCS'04, October 10–13, 2004, Baltimore, Maryland, USA.
Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

1. INTRODUCTION

The importance of information security awareness training should not be underestimated. IAT Services, the central IT group at MU, has implemented a comprehensive security awareness program to educate our users about the importance of information security. This paper will explore the creation of the program, the identification of different audiences and methods of information delivery and how to define what content is vital to a successful program. It will also discuss how to successfully maintain a relevant, long-term information security awareness program.

2. GOALS

The goals for the IATS Security Awareness program are to:

- Change the way people think and act when it comes to information security,
- Develop metrics to measure the level of the audiences knowledge and the success of the program, and
- Continually address the importance of information security in the campus environment.

3. PLANNING

MU developed an information security awareness program for students, faculty and staff. The program aims to educate users and change behavior through two main avenues: security awareness training and monthly activities. The planning process consisted of determining vital content, defining audiences and choosing the correct methods of delivery.

3.1 Determining content

In order to determine content, we first evaluated the security related problems that IATS dealt with on a daily basis. We did this based on tangible statistics, such as reports from our call-tracking system, as well as perceived problems. While talking to people about what they perceived to be our biggest security problems, we realized that some things will always be problems, some things will only be a problem at a specific time, and new problems will always be popping up. Based on this, we decided we were going to have to be flexible with our content so we could incorporate new problems or concerns as they arose. In order to accommodate this need and avoid constantly revising our material, we decided that the training component of our program

would consist of static topics that will be evaluated on a yearly basis, while the monthly activity component of our program would consist of topics that were relevant at the time. Since the monthly activities focus on what is important at the time, the initial focus was on establishing the list of necessary topics for the training.

After we felt that we had a good idea of what should be included in the program, we solicited opinions from managers within IATS, including our desktop support, help desk, server support, networking and training managers. As we suspected, most of the managers were in agreement with us as far as what topics should be covered. However, some of the technical managers felt that we had not included enough specialized information to keep the “techies” interested. Based on this feedback, we re-evaluated our content. In doing so we found what we considered to be a more appropriate balance between technical and non-technical information.

At this point, our list of topics for the training consisted of password safety and security, workstation security, internet and email security, physical security, FERPA (Family Educational Rights and Privacy Act)¹ and HIPAA (Health Insurance Portability and Accountability Act)². We felt this curriculum was a good starting point and covered the majority of the issues IATS deals with on a daily basis, but we decided to take things one step further and evaluate what the information security industry says is vital for end-user education. Doing this opened our eyes to two concepts we had not previously considered: social engineering³ and the principle of least privilege⁴. While neither was perceived as a major problem at MU, we decided we would like to educate our users before they become problems, thus adding these two topics to the training.

For the monthly activities, we came up with an initial list of “hot topics” with the idea that they could be adapted to meet our needs at the time. The initial list consisted of our new password requirements, “All About Updates” (OS and antivirus), DMCA (Digital Millennium Copyright Act)⁵, identity theft and the University’s acceptable use policy.

3.2 Defining audiences

Initially we thought we would have two different audiences – students and faculty/staff. While this is true, we quickly realized that it’s not this simple. We actually have multiple audiences within the two groups and it is likely we will have more than we have recognized thus far.

¹ <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

² <http://www.cms.hhs.gov/hipaa/>

³ http://www.sans.org/rr/catindex.php?cat_id=51

⁴ <http://www.itsecurity.com/dictionary/leastpriv.htm>

⁵ <http://www.copyright.gov/legislation/dmca.pdf>

3.2.1 Students

The broad category of students includes on-campus students living in residence halls and Greek houses and off-campus students. These two subsets of the student population require different methods of delivery, which will be discussed later in this paper.

3.2.2 Faculty/Staff

While most faculty and staff can be lumped into a general category for the purpose of our security awareness program, we recognized early on that many of the faculty and staff in administrative positions, such as deans and department chairs belong in a category of their own. The people in these positions don’t have time to devote to attending a lengthy training class or reading a long article, so we have to consider their needs separately. Getting upper level administrators involved in the security awareness program was vital. With their buy-in, we realized that we would be more likely to have cooperation from the rest of their department.

3.3 Choosing the correct methods of delivery

This particular portion of the planning process was fundamental to the success of our program. We had to consider not only the topics and the appropriate ways to deliver those topics, but we also had to take into account our different audience factions.

3.3.1 Students

We decided on a few of methods of delivery that would work for all students: targeted mass e-mail, articles in our monthly technology newsletter, ads in the student newspaper and presentations to groups or clubs. Additional methods we planned to use to reach on-campus students specifically included posters in residence halls and Greek houses, mailbox stuffers and table tents in dining halls. For off-campus students, we use poster campaigns in the student unions, classroom buildings and frequently visited places such as the library or computing sites, however, we had to keep in mind that exposure is not guaranteed as it is in the residence halls and Greek houses. As a whole, there are some factors that distinguish students from faculty/staff. For instance, we can reach faculty/staff with in-person training that their department coordinates. With students, it is much more difficult to coordinate face-to-face training so we decided to concentrate on web-based training for them.

3.3.2 Faculty/Staff

For faculty and staff, we planned to use in-person and online training, poster campaigns, articles in the monthly technology newsletter, targeted mass e-mails and payroll stuffers. Additionally, we decided to use a concise high-level overview of the training to fulfill requests from administrators and people seeking to fit us into a pre-scheduled meeting.

3.4 Branding

In order to create consistency and recognition, we decided to brand our entire security awareness program with a logo and a theme, which will change on a yearly basis. For 2004, our theme is “You Are The Key to Security!” and our logo is the key figure below.



Figure 1. MU Security Awareness Logo

We use this logo and theme on all of our published material, both hard copy and web-based.

4. IMPLEMENTATION

In the next phase, IATS began implementing the ideas formulated during the planning phase. A comprehensive information security awareness program was created that has two components: topic-specific monthly activities and general information security awareness training.

4.1 Monthly activities

IATS chooses one “hot topic” per month on which we spotlight education efforts. The goal of the monthly topic and the activities promoting it is to increase our user’s knowledge and awareness of that particular information security issue. Also, we hope to get security-related information out to the campus in an organized and consistent fashion.

4.1.1 January monthly topic example

The theme for January was “Password Safety & Security”. This topic was tied to a mandatory, campus-wide password reset campaign that we initiated. The topic was covered in our Security Connections newsletter article (“What’s All The Hype About Passwords?”)⁶. We created a poster that included instructions on changing passwords and listed password best practices. We hung this poster in central student areas, computing sites, residence halls. We also made it

⁶<http://iatservices.missouri.edu/techknowledge/01-2004/security.html>

available to departmental computer support personnel for distribution in their buildings. Furthermore, we sent a mass e-mail to all faculty, staff and students with information on the password reset campaign and general password best practices.

4.1.2 April monthly topic example

April’s topic was “Cyber-Security”. We invited a guest speaker from the Kansas City office of the FBI Cyber Crime Task Force to speak about their various on-going cyber-security efforts. We tailored a presentation to graduate-level business classes that covered general security issues and auditing information. Finally, we created a security awareness website⁷ that included links to and descriptions of various security sites of interest to our campus community.

4.2 Security awareness training

The second component of the security awareness program is our security awareness training course. The material for this course was compiled during the planning stage. This training was first implemented in January of 2004.

4.2.1 In-person training

The core of our security awareness training is currently a one-hour, in-person training class. This class covers a variety of topics, including password safety and security, workstation and physical security, and internet and e-mail security. The course is delivered free of charge to departments and student organizations. The availability of this course was initially advertised to our departmental computer support personnel community, who then contacted IATS when they were ready to schedule their training. The course instructor met with each departmental support person prior to delivering the training to review the material and note any special circumstances that might exist within a particular department. Training was then delivered to the department. Some departments chose to make the training session mandatory and others decided to have it be an optional course. This decision was left to the discretion of the department. Some student groups have also opted to take advantage of the training. These groups have a representative contact IATS to set up a time and location for the class. To date, over 1,100 faculty, staff and students have attended the IATS Security Awareness training class.

⁷ <http://iatservices.missouri.edu/security/awareness/>

4.2.2 *Online training*

Another training option that is currently in development is an online training course created using WebCT⁸ that will be ready to roll out in fall of 2004. This course contains the same information that is contained in the in-person training; however, this delivery method will allow us to reach users not served by traditional training. For example, we have students studying abroad and faculty/staff members at outreach sites across the state. The online course will allow these users to receive security awareness training.

5. FINDINGS

One size does not fit all. When adapting our program to meet our current needs, we were pleased that we had built in flexibility from the beginning. This flexibility allowed us to make changes as necessary without compromising the integrity of the program as a whole. By being flexible with our methods of delivery, we were able to reach more people, and in doing so we realized that the campus community is generally receptive to the program and is happy to be given the opportunity to learn more about information security.

6. PLANS FOR IMPROVEMENT

We hope to work with specific professors (generally, those who teach computer-intensive courses) to make the Web-CT course mandatory for students enrolled in their classes. We also hope to make in-person or online training mandatory for faculty and staff.

Furthermore, we plan to develop policies and procedures that help us adequately address new security threats or issues without having to reinvent the wheel each time.

We hope to continue to identify new methods of delivery, such as working with local apartment complexes that house primarily students to distribute fliers and mailbox stuffers. We are also looking into using pre-defined communities (such as Freshman Interest Groups and Residence Hall Learning Communities) as an avenue of information dissemination.

Since our program is new, metrics are difficult for us to define. For instance, we have seen an increase in reports of computer viruses, but we are unable to link this trend to a specific cause. Are more viruses being circulated on the Internet or has our awareness program led to increased reporting of virus infections? Gathering statistics and trending will allow us to more accurately measure the success of our program.

Finally, we plan to continually revise the current security awareness program to address new topics or issues, with the intent of keeping the program relevant to our user community.

⁸ <http://www.webct.com/index.html>