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.

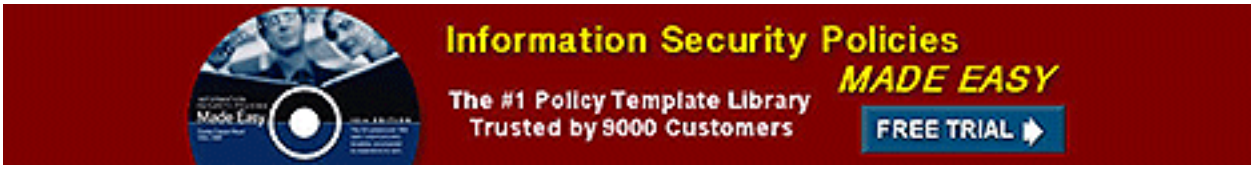
## Social Engineering Your Employees to Information Security

This paper will examine the role and value of Information Security Awareness efforts in the organization. I will discuss the various threats (e.g., social engineering tactics) targeting employees that an InfoSec Awareness campaign is designed to counter. We will review some of the obstacles to implementing a program, offer some tools and strategies for developing effective materials, and lastly look at two case studies of Information Security Awareness campaigns at the University at Albany, SUNY. The appendices contain...

Copyright SANS Institute

Author Retains Full Rights

AD



# Social Engineering Your Employees to Information Security

GSEC

GIAC Gold Paper for Security Essentials

by
Martin Manjak
mm376@albany.edu

©June 1, 2006

© SANS Institute 2006, All Rights Reserved.



© SANS Institute 2006 All Rights Reserved

# Table of Contents

Abstract....4
Document Conventions....4
Section 1: The Role of Employees in Information Security....5
*Introduction*....5
*Infosec: Part of Internal Controls*....5
*Ignorance of Controls; Inadvertent Exposure*....6
*Deliberate Attempts to Subvert Controls*....7
Impersonation & Pulling Rank....8
Conformity....8
Helplessness....8
Surveys....9
Shoulder surfing & Eavesdropping....9
*Values, Roles, & Criteria*....10
Section 2: Obstacles to Educating Employees....12
*Introduction*....12
*Indifference & Ignorance*....12
*Executive Level Buy-in*....13
*Money & Bad Art*....13
Section 3: Identifying At Risk Behaviors and Attitudes....15
*Introduction*....15
*Ask Support & In-House Training Staff*....15
*Gathering First Hand Information: Surveys, Questionnaires, Interviews, and Focus Groups*....16
Surveys....16
Questionnaires....17
A concise list of questionnaire do's and don'ts is summarized in Robert B. Frary's, Hints for Designing Effective Questionnaires.....17
Interviews....17
Focus Groups....18
Section 4: Identifying the Core Message....20
Section 5: Case Studies....22
*Case Study #1: Managing Users of Unmanaged Machines*....22
Fall 2004: Opening Week Melt Down....22
"It's Your Fault!"....23
Communicating with Students: A New Approach....23
Importance of Design....23
Security Quiz: Gateway to Connectivity....24
Results....24
Conclusions....26
*Case Study #2: Making People the Message*....26
Background....26
The Hook....27



© SANS Institute 2006 All Rights Reserved

It's Everybody's Game.....27
Appendices .....29
*Appendix A: Case Study 1—Sample Materials*.....29
*Appendix B: Case Study 2—Sample Materials*.....29
*Appendix C: Sample Survey*.....29
References .....33

© SANS Institute 2006, All Rights Reserved.



© SANS Institute 2006 All Rights Reserved

## Abstract

This paper will examine the role and value of Information Security Awareness efforts in the organization. I will discuss the various threats (e.g., social engineering tactics) targeting employees that an InfoSec Awareness campaign is designed to counter. We will review some of the obstacles to implementing a program, offer some tools and strategies for developing effective materials, and lastly look at two case studies of Information Security Awareness campaigns at the University at Albany, SUNY. The appendices contain samples of actual materials developed using the methods discussed in the paper.

## Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

| | |
|---|---|
| URL | Web URL's are shown in this style. |
| *Quotation* | A citation or quotation from a book or web site is in this style. |

© SANS Institute 2006, All Rights Reserved



© SANS Institute 2006 All Rights Reserved

# Section 1: The Role of Employees in Information Security

## *Introduction*

The success of any enterprise is dependent on a well-informed, dedicated, and ethical work force. This applies in varying degrees to anyone affiliated with your organization: full-time and part-time staff, contract employees, consultants, business partners, and even vendors.

Ideally, information security should be part and parcel of a set of internal controls that govern the processes, operations, and transactions that constitute the life of the organization. These controls should be internalized to the point where an individual would be no more likely to expose the organization to harm than they would themselves, i.e., as routine and habitual as locking the car when leaving it in the parking lot.

Wherever possible, information security should be built into business processes. To accomplish this, information security must be generally recognized and accepted as a distinct value within the institutional culture that informs and influences employee behavior.

The challenges to information security professionals are, first of all, to convince management of this, and second, to develop and carry out the awareness programs needed to inculcate information security as a highly valued attribute and attitude among the work force.

## *InfoSec: Part of Internal Controls*

While the functions and responsibilities of internal auditors and corporation counsel have long been understood and accepted by management, information security professionals do not enjoy the immediate credibility and urgency afforded by management to members of the auditing or legal professions when the latter raise issues of compliance. Information security staff must often make their case from the ground up, despite the fact that their area of concern is as important to the organization's operations as that of audit and counsel. All three offices share the duty of reminding employees of the internal



© SANS Institute 2006 All Rights Reserved

control framework within which they function, and fostering the attitudes that will translate into responsible behaviors with regard to the organization's information and financial assets.

## *Ignorance of Controls; Inadvertent Exposure*

A particularly telling example of what can happen when employees are not familiar with internal controls and information security practices is the story of how the account information for more than 240,000 subscribers of The Boston Globe and the Worcester Telegram and Gazette was exposed.

> *The snafu occurred when the account information of Globe and T&G subscribers who pay for their home delivery subscriptions by credit card was disclosed on the back of more than 9,000 individual routing slips used to label bundles of the Worcester Sunday Telegram, the Globe said in a statement today. The bank routing information of some T&G subscribers who do not pay by credit card may have also been inadvertently disclosed, the paper said.*
>
> *According to the Globe, discarded reports were recycled as paper used to print the routing slips. The newspaper was alerted to the compromise by an employee at a store that sells copies of the newspaper, said Alfred Larkin, senior vice president of general administration and external affairs at The Boston Globe. "As soon as senior management became aware of the situation, we dispatched a significant portion of our delivery force and attempted to recover as many of the routing slips as possible," he said.*
>
> *According to the Globe's account of the incident, data was printed out twice in recent weeks by business office workers at the T&G and then thrown away to be recycled. In one case, an employee started to print a report, stopped the printing before it was done and discarded the paper. In the second, a different employee began printing out a report, realized it was the wrong one, aborted that job and threw the report out.1*

As the report points out, the information on subscribers' accounts was printed out by two different employees who then treated the paper printouts as just another item to be recycled. The employees probably felt they were being conscientious by placing the reports in the recycling bins. No additional value was assigned to this information that would have caused the employees to consider whether placing the reports in the recycling bins was the best way to



© SANS Institute 2006 All Rights Reserved

handle subscribers' financial account data. The employees did not understand the sensitivity of the information, nor their role in preserving its confidentiality.

As a result, the two newspapers found themselves in an extremely embarrassing situation that threatened their continued relationship with a huge customer base, arguably weakened their ability to attract new customers, and left them exposed to expensive legal actions.

While some may argue that the lack of a technical control (limiting employee access to the report) contributed to this scenario, clearly the employees failed to recognize that subscriber account information demanded special treatment on their part.

Technical controls have a role to play in mitigating unauthorized disclosures. In the case above, access controls could have prevented the employees involved from printing the report in the first place. But presuming they had a legitimate business need for this information, they clearly failed to appreciate the potential consequences of its exposure.

### *Deliberate Attempts to Subvert Controls*

Information security cannot rely exclusively on technical or physical controls. Employees have to be trusted to do the right thing if the business is to operate effectively. Further, technical controls will not provide sufficient protection in situations where attackers deliberately try to gain access to information directly from employees.

In the example above, the disclosure occurred accidentally. However, staff must be adequately prepared to resist active attempts to elicit sensitive or confidential information through psychological manipulation, i.e., social engineering attacks. Much has been written about the various ploys and tactics used by attackers to pry information from unwitting employees such as "impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness."[2]

A quick examination of some of these approaches will show that organizations cannot rely solely on technical controls when employees are subject to social engineering attacks.



© SANS Institute 2006 All Rights Reserved

## Impersonation & Pulling Rank

Impersonation involves an attacker assuming the role of an individual who pretends to have some legitimate need for the information the attacker is seeking. The assumed role could be that of an actual employee, or someone outside the organization who purports to have a relationship with the company, or is simply doing some work at the moment for the company (e.g. phone repair).

This can easily evolve into a slightly different tack where the attacker assumes the role of someone in a position of authority, i.e., pulling rank. It doesn't require a precise impersonation of the company officer, just an assumption of that position's authority.

Who among us doesn't want to please the boss, or the boss's administrative assistant? By adopting a high status attitude, the attacker can get what she is looking for, particularly if the attacker encourages employees' propensity to ingratiate themselves with higher ups. If the attacker is particularly skilled, she can leave her victim thinking they just added a few feathers to their cap rather than jeopardizing the entire customer database.

A particularly effective variation of this tactic is to impersonate someone with authority coupled with an urgent situation that requires an immediate response.

## Conformity

Conformity is another powerful social force. If an attacker can convince an employee that everyone else has already performed the actions requested, such as confirming account names and passwords, it becomes very difficult for an individual to resist.

A variation on this theme is diffusion of responsibility. If an attacker can convince his victim that the victim's supervisor has already approved the action, and if the assignment of duties among staff is not clearly delineated, it is possible to fool the employee into revealing the sought-after information.

## Helplessness

Attackers know you can catch more flies with honey than vinegar. A combination of friendliness and helplessness can trigger an outpouring of information, particularly from



© SANS Institute 2006 All Rights Reserved

help desk staff. Help Desk employees are especially vulnerable to individuals who show an appreciation for their assistance. A natural response is to provide even more information when the customer is so eager for, as well as impressed by, your knowledge. By playing dumb and carefully asking leading questions (baiting) based on the real time responses of the help desk agent, an attacker can come away from the encounter with a wealth of information about a company's IT organization.

## Surveys

Surveys are an information gathering instrument tailor made for attackers. They require no special relationship between the attacker and the victim, and are by their very nature designed to elicit information in a question and answer format. Through careful coordination, a team of attackers might be able to prepare employees ahead of time for the survey process and even provide them with permission to disclose sensitive information!

A dramatic example of this occurred in the spring of 2006 when the organization, InfoSecurity Europe <www.infosec.co.uk>, conducted a survey of commuters at Victoria Station in London.[3] Pretending to ask about Easter candy giving habits, the researchers found that they were able to acquire enough personal information from 81% of the respondents to attempt identity theft.

## Shoulder surfing & Eavesdropping

Shoulder surfing and eavesdropping can be very effective in gathering useful information about a company's personnel and operations.

The term shoulder surfing refers to any direct observation of sensitive information such as individuals keying in passwords or PINs, the display of information on computer monitors, or simply personnel forms with SSNs left exposed on someone's desk. Shoulder surfing is no longer limited by the physical presence of the intruder. This technique has been significantly enhanced with the advent of digital imaging using charged coupling devices (CCDs) (RW, what is a CCD? Use it in full with the acronym after then you can use the acronyms safely.) and cell phones equipped with photographic capabilities. An article posted to Bruce Schneier's blog in Sept. of 2005 documents an instance of a thief using a video camera to photograph letter carriers



© SANS Institute 2006 All Rights Reserved

opening letter boxes. The videos were carefully examined and used to create copies of the letter carriers' keys.[4]

Eavesdropping in the context of information security is defined as listening in on conversations among individuals associated with the target organization.

> *In its most basic form, it amounts to one person keeping within earshot of a conversation between two other persons, but in the security and IT worlds it extends to remote listening and recording devices, including the interception of telephone calls, fax transmissions, e-mails, data transmissions, data-scoping, and even radio scanning for mobile communications.*
>
> *The security implications for companies are primarily that user identification details or passwords can become known to criminally inclined individuals, or that confidential/sensitive information about the organization, its finances, or activity plans may leak to competitors.5*

A recent event may serve as a brief example of both. I took my car to a local lube shop for an oil change. While sitting in the waiting room with other customers, I was privy to various customers' personal information, including cell phone numbers and home addresses when they provided them in response to the staff's requests. Additionally, when I went to pay for the work done to my car, I was able to see other customer's records, including names and addresses, displayed on the shop's monitor used to generate invoices.

## *Values, Roles, & Criteria*

As socialized human beings, our initial impulse is to believe what we are told, and respond with help when asked, particularly on the job where a hierarchical social arrangement rules and we are expected to act with a certain measure of professionalism. These tendencies generally benefit the organization, but when exploited by unscrupulous individuals they can be leveraged into significant liabilities. In the examples offered above, the safety of the company's information assets will be determined not by any technical safeguards, but will rely for the most part on the common sense and natural behavioral tendencies of individual employees.



© SANS Institute 2006 All Rights Reserved

Clearly, without an effective information security awareness program, the organization's information is at risk! Information Security awareness programs should provide employees with

- a set of values they can use to make responsible decisions regarding the organization's information assets,
- an understanding of their role in protecting these assets, and,
- criteria that can be employed to assess the legitimacy of requests for access to confidential or sensitive data.

If the employees of the Telegram & Gazette had taken part in an effective Information Security awareness campaign, they would have had the knowledge and tools needed to make the right decision about subscriber account information. In the next section, we'll look at some of the reasons why they didn't.

© SANS Institute 2006, All Rights Reserved



© SANS Institute 2006 All Rights Reserved

# Section 2: Obstacles to Educating Employees

## *Introduction*

This section will examine some of the obstacles to developing and publicizing an Information Security Awareness program. Budgetary constraints, poor design, lack of executive level support, and a fundamental misunderstanding of the real issues can individually and collectively doom any campaign that fails to take them into account. Proper planning and execution are critical just as they are in any project. There is nothing trivial in carrying out an effective Information Security Awareness program. It is a significant undertaking and should be recognized as such from the onset. The following paragraphs will try to identify the major difficulties you can expect to encounter.

## *Indifference & Ignorance*

As Information Security professionals, we have to give our employees a reason to be concerned about good security practices. Before you can address ignorance, you have to attack indifference. Employees will not be motivated to change behaviors if they see no reason to change. So the first task is to raise awareness and convince staff that they have a personal stake in the effort to secure the organization's information assets. Many Information Security professionals make the mistake of viewing the issue of security awareness as a technical problem. Security awareness is not training. It is raising consciousness within the organization of the threats to its well-being and the role employees play in mitigating those threats.

In her article, "Developing Security Education and Awareness Programs,"[6] Shirley Payne identifies the following attitudes among employees that hinder the development of good security practices:

- Lack of understanding of the nature of security threats
- Do not consider it important
- Rely on someone else to take responsibility for security
- Deny any personal responsibility for security
- Consider the issue too technical for them



© SANS Institute 2006 All Rights Reserved

A careful examination of these will reveal that they are interrelated. A lack of understanding of the nature of the threat could easily lead to a belief that the issue is technically beyond one's competence. Denial of personal responsibility contributes to the belief that it's someone else's job, or that it's of little or no importance. All of these must be taken into account when designing materials that are intended to counter these assumptions. Promotion of good security practices can only take place after reversing these negative attitudes.

## *Executive Level Buy-in*

Executive level approval and support is critical to the success of your program on two counts. You must convince your boss that the effort will be worth the expense; and executive support, by virtue of their example and authority, will convey the message to the troops that this is important and requires their attention. Kick off your campaign at the highest level possible. Inaugurate your program with an email from the President or CEO. Preferably, have several members of the executive cabinet endorse your efforts in a highly publicized affair that launches the program. Executive endorsement can pay huge dividends and is well worth any effort on your part to cultivate it.

The opposite also holds true. Lack of executive support will hamper even the most visually engaging campaign. No matter how appealing the material, employees will question how much the message applies to them.

## *Money & Bad Art*

An effective education program requires adequate financing. How much is enough? It will help to view the effort as a public relations campaign, analogous to promoting a product or good public health practices.

Where do you start? With art direction. The value of a professional art director and public relations manager cannot be over estimated. Not only will they design effective, eye-catching pieces, they can also offer invaluable guidance on the overall arc of the campaign, they can manage the production process, and they can provide reliable estimates of the likely costs.



© SANS Institute 2006 All Rights Reserved

You would not want an amateur configuring your organization's firewall. Likewise, you do not want a person inexperienced in running a PR campaign (i.e., you) designing your Security Awareness program. You are a source of valuable information and insight in creating the program, but you need a professional to translate that knowledge into an effective campaign.

A Security Awareness program should be treated no less deliberately and conscientiously than other efforts to secure the organization's information assets. Unlike other forms of controls, however, the expertise in mounting an effective PR campaign will probably lie outside the office charged with Information Security.

It is essential that you come up with a realistic budget before going to your boss for approval. Like any other project, you want to identify all the likely costs up front in order to cover the expense of the campaign and avoid the embarrassment of going over budget. You should probably give your boss a range of budget options. Again, professional PR people can help with developing these figures.

(This is another reason for hiring a good visual designer. If you can come up with a program that looks like it will be popular, the brass will want to be a part of it.)

Before deciding on the topics to be addressed in your Information Security Awareness campaign, it is necessary to find out what employees think about the topic. The next section will suggest some techniques and strategies for doing that.

© SANS Institute 2006, All Rights Reserved.



© SANS Institute 2006 All Rights Reserved

# Section 3: Identifying At Risk Behaviors and Attitudes

## *Introduction*

To effectively counter and discourage the types of behaviors and attitudes that put the organization's information assets at risk, it's necessary to identify them. By targeting specific employee behaviors and attitudes, you can craft much more effective messages to persuade them to change both. The challenge then is to discover just what types of behaviors need to be discouraged and what types of assumptions would result in unwanted risk or exposure of company assets.

This section will discuss some of the ways of gathering this information.

## *Ask Support & In-House Training Staff*

One of the best sources of employee relations with IT is your Help Desk staff and field technicians. They are intimately familiar with the types of things people do with their PCs that get them into trouble. Desktop support personnel that visit and troubleshoot workstations can provide a wealth of anecdotal information about the ways employees interact with technology. They can help you identify and prioritize behaviors that appear to be the source of a large number of problems.

Do some data mining of your Help Desk tracking and reporting software if you aren't already receiving monthly reports. Statistics can reinforce, or contradict, the impressions of Help Desk staff. In either case, they should provide insight into employee actions that lead to increased security risks.

Similarly, if you have in-house training, talk to your instructors. They can provide valuable information about the types of problems or questions they are presented with by regular employees in the course of training sessions. (If employees aren't asking security related questions, but engage in high risk behavior, you know you have your work cut out in trying to build awareness of this issue.)



© SANS Institute 2006 All Rights Reserved

## *Gathering First Hand Information: Surveys, Questionnaires, Interviews, and Focus Groups*

A good way to gauge employee knowledge and attitudes with respect to information security is to ask using surveys, questionnaires, interviews, and focus groups.

### Surveys

*Survey Formulation*
Creating a good survey is a specialized skill, as is selecting a meaningful sample. Get help if you've never done this before. If not executed properly, your data will be unreliable and your conclusions incorrect—a situation that will guarantee failure in designing effective materials.

Some things to take into consideration when formulating a survey are: whether to use quantitative or qualitative units of measure (scalars), how you will tabulate your results, what kinds of demographic information you want to collect.

One of the challenges in developing a survey is creating questions that will gather the information you're seeking without introducing too much bias into the results.

However, if you leave your questions too open-ended, it will be difficult to tabulate your answers with any consistency and draw any conclusions from your data.

A good reference work for creating effective surveys is Customer Surveying, A Guide for Service Managers by Dr. Frederick Van Bennekom, published by Great Books Consulting, http://www.greatbrook.com/survey_guidebook.htm.

*Measures of Success*
A follow-up survey can be a useful measure of the success, or failure, of your Information Security Awareness program. The follow-up can measure both the visibility and impact of your campaign. This holds true for the interviews and focus groups, as well. All these tools can be used to gauge the effectiveness of your efforts, as well as gather initial information about employee attitudes and knowledge.

A sample survey can be found in the appendices of this document.



© SANS Institute 2006 All Rights Reserved

## Questionnaires

Questionnaires are a variation on the survey form of information collection. Although they are similar, a survey is an instrument that should be self-explanatory and requires no additional assistance or input on the part of the researcher for the subject to complete. Ideally, the respondent could complete the survey, whether in paper or web form, entirely on their own.

A questionnaire, while still needing careful formatting and structure, presumes the presence of the researcher and should allow for more flexibility in collecting and recording responses than a survey.

A questionnaire can let the employee expand on their answers and gives the researcher the opportunity to hone in on certain topics as opportunities present themselves in the more dynamic setting of a live, synchronous exchange between the subject and researcher.

A concise list of questionnaire do's and don'ts is summarized in Robert B. Frary's, Hints for Designing Effective Questionnaires.[7]

## Interviews

A series of interviews offers an opportunity to get a very in-depth look at employee's attitudes, assumptions, and knowledge of a topic. Interviews can be used as follow-ups to information already collected by your survey or questionnaire.

Although interviews should be structured, they are much more open-ended than the previous two instruments. As might be expected, interviews require a special approach since they are more personal in nature.

There are several different types of interviews as identified by Carter McNamara in his General Guidelines for Conducting Interviews.[8] They include:

- Informal, conversational interview: The least structured of the four types of interviews. Requires considerable skill and experience on the part of the interviewer. Can ferret out good information, but difficult to correlate and compare with other subjects' responses because of the lack of comparable structure from one interview to the next.



© SANS Institute 2006 All Rights Reserved

- General interview guide approach: the interviewer proceeds from a set of guidelines. Still very flexible, but offers a road map for all the interviews in the series to allow for some comparison of answers.
- Standardized, open-ended interview: All respondents are asked that same set of open-ended questions. Similar to administering a questionnaire, but the responses are not standardized. Allows for quick interviews that more readily lend themselves to analysis.
- Closed, fixed-response interview: Essentially the same as administering a questionnaire with standardized responses that the subject must chose from.

Since the respondents themselves are not recording their answers, it is crucial to make provisions for accurate record keeping in an interview.

## Focus Groups

Focus groups bring people together and create a group dynamic around a topic or issue. The major advantage of focus groups over interviews is the synergy generated by the group's discussion of the topic. As individuals share their knowledge, attitudes, and feelings about a subject, they will elicit responses from other members of the group, both to the topic itself and to other participants' input.

If carefully facilitated, this can lead to a greater understanding of the subject on the part of all participants, including the researchers. The extent to which the subjects will reinforce, challenge, or modify their own and other participants' assumptions will provide valuable insight to the researchers about the core beliefs and knowledge held by the participants.

Success in hosting a focus group depends on providing a comfortable environment, a well considered set of questions, and the skill of the facilitator in creating a positive group dynamic and leading the group through the questions.

As is the case with interviews, it is vitally important to keep good records of people's responses.

Additional advice on preparing, developing, planning, and facilitating effective focus groups can be found in Carter McNamara's Basics of Conducting Focus Groups.[9]



© SANS Institute 2006 All Rights Reserved

In the case of all these instruments, surveys, questionnaires, interviews, and focus groups, you will need executive level support. Employee participation in these efforts will be much easier to obtain with the endorsement of management.

© SANS Institute 2006, All Rights Reserved.



© SANS Institute 2006 All Rights Reserved

## Section 4: Identifying the Core Message

Armed with the results of your surveys and other efforts to ascertain your employees' attitudes towards Information Security, you can start to identify the issues you want to address in your awareness campaign. Before developing the actual materials, it is important to determine what the core message will be. Are you looking to promote awareness of organizational policies, standards, or values? Do you want to remind employees of the consequences for violating company policies? Do you want to heighten awareness of the threats to your organization? Are you going to focus on specific behaviors, stigmatizing and discouraging those behaviors that put the organization at risk or promoting those behaviors that enhance your information security posture?

Look for an overriding theme that can tie all the materials together and create a branding mark, a catch phrase or slogan, or a look or icon that will provide instant recognition for your campaign and highlight its central message.

It's worth repeating that Information Security Awareness is not training. You should avoid detailed technical explanations or how-to descriptions in your awareness materials. The intent is to quickly grab people's attention in whatever format you are using (posters, newsletters, flyers, bookmarks, refrigerator magnets) and hit them with the message. Think in terms of action words. What do you want your employees to **do** or **not do** as a result of encountering your Information Security awareness publications?

If you can reduce the message to an action, it will serve as a focal point for the design of your materials.

In many respects, text is your enemy. There is an inverse ratio between the amount of text used and the effectiveness of your communication. Use the visual element to get your audience's attention and convey the brunt of the message. The text should expand on the image and the image should support the text.

However, not every topic lends itself to this kind of treatment. More complex issues do not translate well into posters and require additional explanation. In these



© SANS Institute 2006 All Rights Reserved

cases, try to tell a story. As human beings, we construct reality through narrative. Stories engage us more readily than mere facts. Bullets may summarize key points, but narrative will give those points personal meaning for your employees.

The remainder of this paper will offer examples of the strategies and tools discussed above, along with two case studies of Information Security Awareness campaigns at the University at Albany.

© SANS Institute 2006, All Rights Reserved



© SANS Institute 2006 All Rights Reserved

# Section 5: Case Studies

## *Case Study #1: Managing Users of Unmanaged Machines*

### Fall 2004: Opening Week Melt Down

Late August and early September are make-or-break moments for many institutions of higher learning. This is the time when tens of thousands of students return to campus residence halls with their personal computers. The sudden arrival of these unmanaged machines and the eagerness of their owners to connect them to institutional networks are rightly viewed by network managers, help desk staff, and security personnel as a call to battle stations. It is not unlike the experience many townspeople must have felt when they discovered Attila camped outside the city walls.

The events in the fall of 2003 illustrate this point. Blaster and Welchia were propagating with blinding speed causing many schools to completely shut down their networks and spend weeks going from room to room with CDs to remove the worms and install the MS patch for the RPC DCOM vulnerability one system at a time.

The University at Albany, however, escaped largely unharmed. A quick response by a creative crew of student and professional employees enabled the University to identify infected machines, put them in a network quarantine, and offer a self-remediation process via the web. From the perspective of central IT and management, the Windows RPC DCOM exploits of fall 2003 were non-events on the UAlbany campus.

That was not to be the case in 2004. Beginning with the fall semester, the University began scanning ResNet machines for a variety of exploits. We found them—in significant numbers!

By the end of the first day of fall check-in, over 486 machines had been identified as hacked and were suspended from the network. (UAlbany requires students to register their computers . The campus uses a form of NetReg, "an automated system that that requires and unknown DHCP client to register their hardware before gaining full network access."[10] Suspensions were accomplished by denying DHCP leases to compromised computers.) At its worst point, over 800 machines, approx. 17% of all connected systems, were



© SANS Institute 2006 All Rights Reserved

suspended. The Student Help Desk (SHeD) had over 1000 open tickets the first week of class. There was a 3 week wait for a remediation appointment. Students were lined up outside the SHeD waiting to make appointments, parents were calling the President's and CIO's office, and SHeD staff were threatened with physical violence. As one student employee put it, "Today was the worst day in the history of the Internet!"

## "It's Your Fault!"

Very quickly, two common themes emerged in our dealings with students and parents. The first was that it was our fault that their computers were compromised. In many cases, students were connecting brand new systems to the network straight out of the box. From their perspective, a brand new machine should be clean, and if it wasn't, it was because our network infected their pristine PC.

It also became very obvious that parents and students did not read the letter we had sent to everyone informing them of the steps they needed to perform to secure their computer before they brought it to campus (e.g. installing XP SP2). There was little, if any, understanding on their part of their role in protecting their machines.

## Communicating with Students: A New Approach

It was clear that our efforts to communicate best practices to our students were a failure. Our assumption that students would want to secure their machines was based on the premise that they understood the threats. This turned out to be false. Consequently, we had to re-examine both the methods we used to communicate with students and the formats. We had to shift our message from "you need to do this" to "did you hear the story about…" The focus had to turn away from technology in favor of people and behaviors. We had to create, visually and textually, narratives with which students would self identify. This could best be summed up by saying we started working with pictures of young people, not screen shots. Instead of "how to," we need to convince them "why."

## Importance of Design

An effective design was critical to the success of this effort. We decided to develop a series of materials that would share a common look. That look would prominently



© SANS Institute 2006 All Rights Reserved

feature young people that were representative of our student body.

By creating a series of materials, we hoped to generate a cumulative interest on the part of parents and students. Because the materials were visually and thematically similar, but not identical, we hoped people would want to see all the items in the series.

We also used some of the materials (a series of brochures distributed during summer planning conferences) to stimulate interest in other materials (a Network Survival Kit that would be distributed at fall check-in).

Finally, we took the advice of one of our student employees who suggested we jettison the letter we normally sent to students prior to check-in in favor of a postcard. The advantages of a postcard were many. We could design one that was consistent with the visual look of our other materials, it was cheaper to mail (although more expensive to produce), and the combination of the graphics and the fact that you didn't have to open it made it more likely that it would be read.

Samples of these items are available in .pdf format in this paper's appendices.

## Security Quiz: Gateway to Connectivity

As mentioned earlier, UAlbany employs a version of NetReg that requires students to register their devices before they are allowed unrestricted access to the Internet. One of the gates they must pass through in this process is an on-line quiz that tests their knowledge of computing ethics.

It was decided to add a series of security questions to the quiz that focused on the Six Steps to a Secure PC that we were advocating all student practice. This requirement was announced to students on the postcard we sent them. Forcing students through this hurdle made it unmistakably clear to them that we were serious our security requirements and their responsibilities in this area.

## Results

Student employees of the SHeD who survived the fall 2004 opening approached the start of the fall 2005 term with a certain amount of trepidation. No one knew how effective



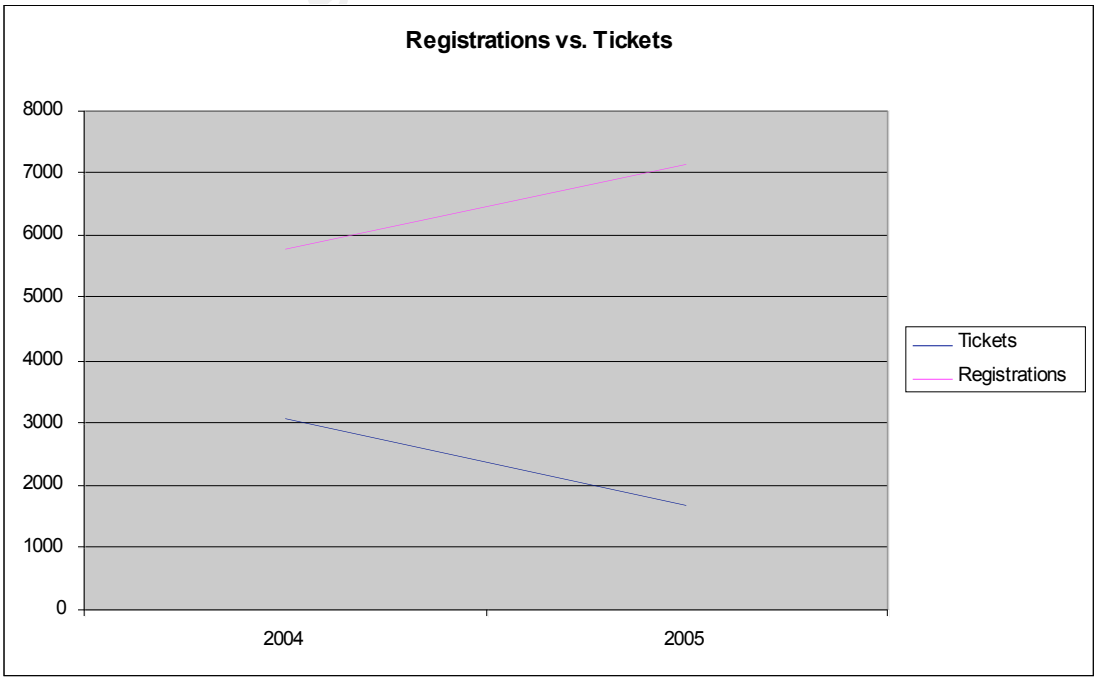
© SANS Institute 2006 All Rights Reserved

our efforts to communicate good security practices to students had been. We were all prepared for the worst as students began arriving and connecting their PCs on opening week-end, and we began scanning.

As it turned out, the fall 2005 start-up was nothing like its 2004 predecessor. With one eye on the ticket counts and the other on the daily registration totals, we saw our registration numbers exceed all previous rates while the trouble ticket count stayed near 100, a very manageable number. The following table compares trouble ticket activity for a period of six weeks, from 08/18 to 09/30 from 2004 to 2005.

| **Ticket Counts** | **2004** | **2005** |
|---|---|---|
| Worked on | 3057 | 1681 |
| Opened | 2967 | 1613 |
| Closed | 2836 | 1586 |
| To Telecom | 36 | 50 |
| Email | 2321 | 1073 |
| Phone/Walk in | 646 | 540 |

This table tells only half the story. To fully appreciate the turn around from 2004 to 2005, not only did we have fewer trouble tickets, we also had more students register. The following graph compares registrations against trouble tickets for the two fall openings.






© SANS Institute 2006 All Rights Reserved

- 5787 machines registered in 2004
- 7140 machines registered in 2005
- 23% Increase in registered systems
- 1376 fewer tickets; or a 45% decrease in tickets

### Conclusions

The absence of malware on students' machines for the fall 2005 check-in cannot be entirely attributed to our education and awareness efforts. The presence of XP SP2 as part of OEM installs was a major factor in reducing the number of compromised machines. The unpleasant experience that many students had in the fall of 2004 likely served as negative reinforcement for keeping their machines clean a year later. The preceding year also saw an increased awareness of computer security among the population in general due to several high profile incidents.

However, based on our contacts with students and some surveys conducted as part of class assignments, students were generally more aware of the University's security requirements and their responsibility in keeping their machines clean. We would like to think that our awareness campaign was at least partly responsible for this.

## *Case Study #2: Making People the Message*

If your target audience is your employees, then make your employees carry the message. In the spring of 2006, the University at Albany embarked on a major effort to heighten awareness of information security risks and best practices among faculty and staff.

### Background

Enterprise systems run by central IT, where Information Security was a paramount value, were well managed, but individual workstations outside of Information Technology Services (ITS) were routinely the victims of attacks. Further, ITS was only one of several information technology providers on campus. Many individual colleges and departments provided IT services in-house.

College campuses typically are defined by three broad populations: students, faculty and staff. Leaving aside the student population, campuses can be divided into two camps, one ruled by a culture of academic freedom, enquiry,



© SANS Institute 2006 All Rights Reserved

and independence, and one that is focused on the business operations of the institution. Traditionally, business operations are more amenable to centralized solutions. The academic side of the house prides itself on its idiosyncrasy. This makes it difficult to enforce standards across the campus.

Consequently, many employees enjoy administrator level privileges on their personal computers. Based on anecdotal reports and Help Desk statistics, we knew that many of the security incidents were due to employees engaging in at-risk behavior with respect to their computers. In the absence of centralized management of systems and the political impetus to reduce end-user rights, there was an urgent need to raise awareness of information security threats and responsibilities among University staff at all levels.

A task force, representing various campus stakeholders, was created and charged with the task of developing ways to communicate information security standards and practices to the campus community.

## The Hook

The University recently experienced its first major intercollegiate championship winning the NCAA America East conference in basketball. One of the members of the task force suggested recruiting famous alumni to help convey the message of information security. This idea evolved into a campaign that would capitalize on the success of the basketball team. The group quickly realized that there would be more value in working with the Athletics Department to highlight student players from *all* the school's intercollegiate teams. What emerged was a campaign based on the theme "Information Security: It's Everybody's Game."

## It's Everybody's Game

The campaign would consist of a series of posters, two per month, to run during the academic year, featuring photos of employees paired up with student athletes. The intention was to invest information security practices with the qualities associated with sports, e.g., active, competitive, worth fighting for with winners and losers, and requiring a collective effort.



© SANS Institute 2006 All Rights Reserved

The participation of the Athletics Department was assured when they were convinced that the campaign would provide exposure for the full spectrum of intercollegiate teams, both men's and women's, across the entire campus. Employees representing both faculty and administrative staff were recruited to participate in the campaign.

Each poster would focus on a specific information security threat and countermeasure, taking into account employee attitudes and knowledge of the subject obtained from a survey distributed to staff. A significant "win" occurred early in our efforts when we convinced the president and the VP of athletics to appear together in the kick-off poster.

This program is still in the design and development phase of the spring of 2006, but a sample of the planned first poster is attached in the appendices.

© SANS Institute 2006, All Rights Reserved.



© SANS Institute 2006 All Rights Reserved

# Appendices

## *Appendix A: Case Study 1—Sample Materials*

## *Appendix B: Case Study 2—Sample Materials*

## *Appendix C: Sample Survey*

### UA Information Security Survey

**Demographics**

1. Are you: Faculty Professional Staff CSEA MC

2. Are you: Male/Female

3. How many years have you worked for the University? <1 1-3 3-5 5-10 >10

4. Do you supervise other UA employees: Yes/No If yes, how many ____

5. In your work, do you handle any of the following records (circle all that apply):

   a. Student IDs/SSNs b. Faculty/Staff IDs/SSNs c. Student Academics

   d. Student Financials e. HR Related f. Research data

**Security Responsibilities**

6. Who is responsible for information security at the University at Albany (circle all that apply):

   A. ITS
   B. Local Technology Support Staff
   C. Individual departments that use the data
   D. Supervisors
   E. Individual employees

7. Who is responsible for the **initial** security configuration of your computer at work? (circle one)

   A. ITS staff
   B. Local Technology Support Staff
   C. My Supervisor
   D. I am

8. Who is responsible for maintaining the **ongoing** security of your work computer? (circle all that apply)

   A. ITS staff
   B. Local Technology Support Staff
   C. My Supervisor
   D. I am



© SANS Institute 2006 All Rights Reserved

**Best Practices**

9. You need to provide information containing names matched to social security numbers to another office. What is an appropriate method for sending this information? (Circle all that apply.)

   A. E-mail message
   B. Fax
   C. Phone
   D. Putting it on a shared drive
   E. Inter-campus mail

10. Your office handles paper documents containing sensitive personal information (names, social security numbers, addresses, grades, etc.). Which of the following statements best describes how these documents are handled?

    A. Documents are not handled in any special manner.
    B. Documents are subject to internal controls and policies to protect confidentiality of information.

11. When leaving for lunch or to take a break, how do you secure your workstation?

    A. Turn my monitor off
    B. Logging off of the workstation
    C. Lock the workstation by pressing control+alt+delete and selecting "lock computer"
    D. Turn the computer off
    E. Other _____
    F. None of the above

12. If someone e-mails you an attachment/link that is not work related, how likely are you to click on it/open it?

    A. Not likely
    B. Somewhat likely, depending on what is being sent
    C. Very likely
    D. Always

13. On average, how frequently are high priority patches/upgrades released for Microsoft products?

    A. Once per year
    B. Once every six months
    C. Once per month
    D. Once every two weeks
    E. Not sure

**Use of University PCs**

14. How likely are you to install desktop weather software on your computer? This either shows up as a webpage when you start your computer, or as an icon in your system tray notifying you of current weather conditions.

    A. Not likely
    B. Somewhat likely
    C. Very likely
    D. It's running on my desktop now.



© SANS Institute 2006 All Rights Reserved

15. Do you have an instant messaging program installed on your work computer? Examples of this include AOL Instant Messenger, Yahoo messenger, MSN messenger, etc)

    A. Yes
    B. No

16. How do you decide to install additional or cosmetic software on your work PC? (Circle all that apply)

    A. Web searches
    B. Online advertising (banner ads or pop-ups)
    C. Advice or recommendation from co-workers
    D. E-mail solicitations

**Current PC Health**

17. Do you currently receive pop-up advertising while browsing the web?

    A. Yes
    B. No

18. Do you have multiple toolbars displayed on your web browser?

    A. Yes
    B. No
    C. Not sure

19. Does your web browser pop up even though you did not start the program yourself?

    A. Yes
    B. No

20. Does your computer seem excessively slow compared to when you first started using it?

    A. Yes
    B. No

21. Has your web browser's default home page changed even though you did not make the change yourself?

    A. Yes
    B. No

**General Security**

22. Sensitive information is stored on my computer?

    A. This is often the case.
    B. This is sometimes the case.
    C. This is never the case
    D. I'm not sure

23. I can play a significant role in protection my computer and the information stored on it.

    A. Strongly agree.
    B. Agree.
    C. Not sure.
    D. Disagree
    E. Strongly disagree



© SANS Institute 2006 All Rights Reserved

24. There is nothing on my work computer that would be of any interest or value to hackers or cyber criminals.

    A. Strongly agree
    B. Agree
    C. Not sure
    D. Disagree
    E. Strongly disagree

25. Installing non-work related software found on the Internet can pose a threat to the confidentiality of information stored on my computer.

    A. Strongly agree
    B. Agree
    C. Not sure
    D. Disagree
    E. Strongly disagree

26. In your opinion, how serious a threat does each of the following pose to the *confidentiality or privacy* of the information stored on your work computer? (Please rate each item by circling one of the choices.)

| | | | | | |
|---|---|---|---|---|---|
| Animated cursors (e.g., Talking Homer) | Not a threat | small threat | moderate threat | serious threat | No opinion |
| Outlook stationery (Smileys) | Not a threat | small threat | moderate threat | serious threat | No opinion |
| Wallpaper | Not a threat | small threat | moderate threat | serious threat | No opinion |
| Extra web search toolbars | Not a threat | small threat | moderate threat | serious threat | No opinion |
| Google desktop | Not a threat | small threat | moderate threat | serious threat | No opinion |
| Unverified Internet software | Not a threat | small threat | moderate threat | serious threat | No opinion |
| Free games | Not a threat | small threat | moderate threat | serious threat | No opinion |
| Downloaded screen savers | Not a threat | small threat | moderate threat | serious threat | No opinion |

© SANS Institute 2006, All Rights Reserved.



© SANS Institute 2006 All Rights Reserved

# References

[1] Vijayan, Jaikumar. "Security snafu at *Boston Globe* exposes subscriber data." Computerworld. Feb. 1, 2006. <http://www.computerworld.com/securitytopics/security/story/0,10801,108268,00.html?from=story_package>

[2] Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." Security Focus. Dec. 18, 2001. <http://wwwsecurityfocus.com/infocus/1527>

[3] "Easter Eggs Bypass Security." InfoSecurity Europe, April 18, 2006. <http://www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=255>

[4] Scheier, Bruce. "Shoulder Surfing Keys." Scheier on Security, Sept. 7, 2005. <http://www.schneier.com/blog/archives/2005/09/shoulder_surfin.html>

[5] "Eavesdropping." Information Security Glossary, RUsecure Security Policy Site. <http://www.yourwindow.to/information-security/gl_eavesdropping.htm >

[6] Payne, Shirley. "Developing Security Education and Awareness Programs." Educause Quarterly, Number 4, 2003.

[7] Frary, Robert B. "Hints for Designing Effective Questionnaires" Practical Assessment, Research & Evaluation 5(3). 1996. <http://www.cmu.edu/teaching/assessment/resources/SurveyGuidelines.pdf>

[8] McNamara, Carter. "General Guidelines for Conduction Interviews." Authenticity Consulting, LLC. 1999. <http://www.managementhelp.org/evaluatn/intrview.htm>

[9] McNamara, Carter. "Basics of Conduction Focus Groups." Authenticity Consulting, LLC. 1999. <http://www.managementhelp.org/evaluatn/focusgrp.htm>

[10] Valian, Peter. "NetReg." NetReg.org. 1999-2005. <http://netreg.org/>

© SANS Institute 2006, All Rights Reserved.



© SANS Institute 2006 All Rights Reserved

Last Updated: November 30th, 2015

# Upcoming SANS Training

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

| | | | |
|---|---|---|---|
| **SANS Cyber Defense Initiative 2015** | **Washington, DCUS** | **Dec 12, 2015 - Dec 19, 2015** | **Live Event** |
| **SANS Dubai 2016** | **Dubai, AE** | **Jan 09, 2016 - Jan 14, 2016** | **Live Event** |
| **SANS Las Vegas 2016** | **Las Vegas, NVUS** | **Jan 09, 2016 - Jan 14, 2016** | **Live Event** |
| **SANS Cyber Defence Delhi 2016** | **Delhi, IN** | **Jan 11, 2016 - Jan 22, 2016** | **Live Event** |
| **SANS Brussels Winter 2016** | **Brussels, BE** | **Jan 18, 2016 - Jan 23, 2016** | **Live Event** |
| **SANS Security East 2016** | **New Orleans, LAUS** | **Jan 25, 2016 - Jan 30, 2016** | **Live Event** |
| **SANS Copenhagen 2016** | **Copenhagen, DK** | **Feb 01, 2016 - Feb 06, 2016** | **Live Event** |
| **Cyber Threat Intelligence Summit & Training** | **Alexandria, VAUS** | **Feb 03, 2016 - Feb 10, 2016** | **Live Event** |
| **SANS Scottsdale 2016** | **Scottsdale, AZUS** | **Feb 08, 2016 - Feb 13, 2016** | **Live Event** |
| **SANS McLean 2016** | **McLean, VAUS** | **Feb 15, 2016 - Feb 20, 2016** | **Live Event** |
| **SANS Secure Japan 2016** | **Tokyo, JP** | **Feb 15, 2016 - Feb 20, 2016** | **Live Event** |
| **SANS Munich Winter 2016** | **Munich, DE** | **Feb 15, 2016 - Feb 20, 2016** | **Live Event** |
| **ICS Security Summit & Training** | **Orlando, FLUS** | **Feb 16, 2016 - Feb 23, 2016** | **Live Event** |
| **SANS Secure India 2016** | **Bangalore, IN** | **Feb 22, 2016 - Mar 05, 2016** | **Live Event** |
| **SANS Anaheim 2016** | **Anaheim, CAUS** | **Feb 22, 2016 - Feb 27, 2016** | **Live Event** |
| **RSA Conference 2016** | **San Francisco, CAUS** | **Feb 28, 2016 - Feb 29, 2016** | **Live Event** |
| **SANS London Spring 2016** | **London, GB** | **Feb 29, 2016 - Mar 05, 2016** | **Live Event** |
| **SANS Philadelphia 2016** | **Philadelphia, PAUS** | **Feb 29, 2016 - Mar 05, 2016** | **Live Event** |
| **Security Leadership Summit & Training** | **OnlineTXUS** | **Dec 03, 2015 - Dec 10, 2015** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |