



Awareness Advisor

Volume 1, Issue 2, Winter 2008

A Complement to Volume 1, Issue 2 of "Protecting Information"
Rebecca Herold, CISSP, CIPP, CISM, CISA, FLMI

My goal.....	1
This quarter’s topic: Social Engineering	1
Social engineering testing	2
How to get the most value from “Protecting Information”.....	3
Provide it in many ways	4
Personalize it to your organization	4
Reward your personnel.....	5
Establish metrics.....	6
References for the feature article	7
A practitioner’s view.....	7
Let me know what you think!	8

My goal

Thank you for subscribing to “Protecting Information” and using it in your organization to raise the awareness and understanding of information security and privacy issues for everyone within your organization. Welcome to my second issue of “Awareness Advisor.” My goal is to provide tips and suggestions to help you use this quarter’s issue of “Protecting Information” most effectively, along with helping in your overall information security efforts.

This quarter’s topic: Social Engineering

The topic of social engineering is important for information security, privacy and compliance leaders to address for many reasons. Most organizations spend the lion’s share of their annual information security and/or IT budgets on technology-based security. However, firewalls, routers, locks, biometrics and even encryption can be defeated by attackers targeting your personnel and getting them to unknowingly help the social engineers with their crimes.

A large portion of information security incidents and privacy breaches occur because too few organizations properly address the human element of information security. The human factor truly is the weakest link in your information security program. The pressure to constantly improve customer service exacerbates the vulnerabilities as personnel strive to hit higher customer service scores and retain business. Personnel must know how social engineering scam artists use deceptive and manipulative tactics to gain unauthorized access to information. Information security and privacy professionals must provide guidance in how to spot and defeat social engineering attempts in ways that are in harmony with customer service goals, and must work with the customer service



management to ensure customer service training includes content for how to spot social engineering.

Personnel also often unknowingly reveal confidential information. For example, if one of your personnel is riding home on a crowded bus and says, “We’re fixing a problem with our online e-commerce program that could let people get access to our customer database,” he or she has just let others within earshot know information they could now use to social engineer their way into your network. That information could be used to plan attacks against the web server, as well as to help social engineer criminals make calls to your organization for further information.

Some of the best tools for preventing social engineering attacks are security awareness training and social engineering testing. The effectiveness of these controls will vary based on the quality of their implementation, including follow-up and retraining. Protection Information will provide the awareness your personnel need to help them identify social engineering attempts and keep incidents from occurring within your organization, and within their own homes. You can provide training using the concepts provided, in addition to follow-up awareness communications. Following your training you can do some social engineering testing to help indicate the effectiveness of your social engineering awareness and training efforts.

Social engineering testing

Social engineering testing, by its very nature, can be difficult to conduct without third-party assistance.

- It can be hard, in organizations where the information security and/or privacy leaders are well known, to have someone from those departments to believably convince personnel they are not from within the organization.
- Many folks do not want to perform social engineering tests with people that they want to happily and cooperatively work with following the tests; they do not want personnel to always be wondering if they are being tested.
- Many, if not most, information security and privacy leaders may feel uncomfortable doing social engineering testing activities themselves, or doing the social engineering training.
- Most information security and privacy leaders don’t have a training background, or are limited in the time it takes to create good, effective training. Because of this a large percentage of organizations do a poor job managing the human element of information security.

One option for social engineering testing is to engage an outside information security and/or privacy consultancy to conduct the testing. There are many organizations that provide this service; I did a Google search on “social engineering” and “testing” and got 950,000 hits. Of course, not all of these were companies that do social engineering testing, but a large number of them was. This outside, objective perspective can enhance the effectiveness of the testing and can uncover areas in which an organization is most vulnerable. The results of the test can then allow for risk to be more accurately assessed and more effective mitigation strategies can be formulated and implemented.



A meaningful social engineering test should involve people who are knowledgeable about social engineering techniques and are creative enough to mimic the methods of real social engineering criminals. Such tests should occur through the coordination of information security, privacy and internal audit departments. The CEO, and perhaps the executive leaders of the business unit being tested, should approve of the testing, and they should not give advance notice to the areas being tested.

Testers should use the same concepts that social engineering criminals make use of:

- Familiarity. The social engineering criminal will often make advance contact within someone in the organization, within an email or in person. For example, they may send an email to a specific person in your organization asking about your products and services, or signing up for some type of communications your organization provides. In person the criminals will often hang around outside your building, be friendly to passers-by, and get to know your personnel. Once personnel have heard from or seen people, they are usually no longer viewed as a complete stranger and, as a result, not viewed as a threat.
- Sympathy. The social engineering criminal will often seem distressed or in need of help. Good social engineering criminals know how to get people to feel sorry for them, and even offer to help them in ways that put your business, or the employee, at risk.
- Comfort and Trust. Once the social engineering criminal is familiar and/or has established a sympathetic perspective from your personnel, it is easier to establish comfort and trust with your personnel. Once the social engineer sees that comfort and trust, the crime is executed.

NOTE: Such social engineering testing activities can open up some significant employee relations issues and sensitivities. Social engineering testing activities should be used to assist with training and awareness, not with the intent of disciplining employees.

How to get the most value from “Protecting Information”

Making “Protecting Information” available to all your personnel is one way in which you will raise the awareness of your personnel about social engineering risks and get them to understand social engineering scams and recognize them when they are attempted. To be effective in getting your personnel to protect information security and privacy at work you must also show them how the actions can also be used within their personal lives to protect themselves, their family and friends. Doing this establishes a sense of responsibility within personnel for them to protect themselves, and their employer, from social engineering threats. It also allows your personnel to take ownership of the issues and feel empowered to not only help your organization, but also their family and friends.



Provide it in many ways

I state this in each issue of Awareness Advisor because it is worth repeating. I recommend you make “Protecting Information” available to your personnel in a number of ways to be able to reach and impact the most personnel possible.

- On your intranet site as HTML
- As a PDF that they can print and take home and share with their family
- Using the accompanying MP3 file
- By encouraging interaction through the review questions

Why provide it in multiple ways? Because there are three kinds of learners, and if you don't communicate to all three kinds your message will not be getting through to everyone. I talk about this in each Awareness Advisor, but it is certainly worth repeating.

There are:

- Visual learners
- Audio learners
- Kinesthetic (hands on) learners

Be aware that most awareness communications are created only for visual learners. By providing the MP3 (podcast) file, along with providing the review (hands on) activities, you will reach what could be a significant portion of your personnel that may never have been reached before.

Consider putting Table 1, “22 Common Social Engineering Schemes” into a hard-copy poster or a card that personnel can post within each of their individual work areas where they can constantly be reminded about the types of social engineering that exist.

You can also put Table 1, “22 Common Social Engineering Schemes” onto your information security and privacy intranet site. If you choose to do this, be sure to include the following citation:

© 2008 Rebecca Herold, "Protecting Information," Volume 1, Issue 2, Information Shield, January 2008.

Personalize it to your organization

Another goal I have with this awareness resource is to provide an opportunity for you to be clearly recognized as the information security and privacy authority within your organization. I want your personnel to go to you and your area with concerns, questions and ideas related to information security and privacy.

With this in mind there are many places within the HTML and PDF for you to personalize “Protecting Information” to your specific organization, and to your own office. Be sure that you make changes in the following locations:

1. Page 1: You can replace the “Information Shield” logo with your own organization's logo.
2. Page 1: Replace “your company president” with whatever your company's leader is called. Or, put the CIO, CISO, or whatever other position is one that all your



personnel would recognize and would feel obliged to give information to under such a situation. You could also modify the example provided to be more in line with your company's business.

3. Page 2: In the title of the article, replace, "Company X" with your organization's name.
4. Page 2: Put your name and title in the "By" line under the title.
5. Page 2: Modify the article, and especially the items in the list, to be appropriate to your organization.
6. Page 6: Change the URL to where your personnel can download the MP3 audio file. You can have them download it from the Information Shield site, or if you have such downloads blocked use a URL from your own intranet.
7. Page 8: If you already have definitions for some of the terms in the "Terms You Should Know" section, either replace them in the newsletter with the definitions your organization uses or, if you like these definitions better, replace your organization's definitions with these.
8. Page 9: Put any additional references in this list that you want your personnel to know about. For instance, to your information security and privacy policies, to an internal information security and privacy news site you maintain, and so on.
9. Page 9: Put your company's name within the indicated location.
10. Page 9: Keep the items that are applicable to your organization. Add any other items that are specific to your organization.
11. Page 10: In item 7, put the person, position, email address, and/or phone number for the person to whom personnel should report social engineering attempts.
12. Page 10: Put the appropriate name and contact information in the paragraph directing employees where to go with concerns.
13. Page 10: Put the URL link or name of your policies manual in the paragraph pointing readers to your policies.
14. Page 10: Put the name and contact information, along with the deadline, for the review question submissions. Also describe the prize for those who answer questions 3 and 4 correctly.
15. Page 10: Change question 4 to be applicable to your organization, as indicated.

Reward your personnel

Here are some prizes for you to consider for your personnel who submit answers to your questions:

- **Memo pads**. Create memo pads with a logo of your information security or privacy mascot, or a slogan, to give to those submitting answers. These can be made fairly inexpensively, and, if you are a non-profit, you can often get donations of such memos, modified to your specifications, from outside organizations.
- **Calendar**. Give those submitting answers calendars with security and/or privacy slogans or themes. There are several downloadable monthly calendars available that you can find quickly with an Internet search. And I'm creating an information security and privacy day-by-day desktop calendar for 2009.
- **Gift card to a book store**. Most personnel love to get a \$5, \$10 or \$25 gift card to a local book store where they can choose what to purchase themselves. You could have a drawing from the correct answers to questions 3 and 4 for the gift cards.



- **DVD.** Have a drawing from those providing correct answers to questions 3 and 4 for a DVD that has a link to social engineering. A great one would be “Catch Me If You Can,” starring Leonardo Dicaprio, about one of the most famous social engineers in history, Frank Abagnale. Another good option would be “Takedown” about Kevin Mitnick.

In previous issues I also provided the following ideas (you can get the details for these from within the previous issues):

- **A “casual day” or “jeans day” whenever the employees choose.**
- **Lunch with the CIO, CEO, or other executive leader.**
- **Coupon for a discount or free meal to your cafeteria or a local eatery.**
- **Half-day of vacation.**

Establish metrics

It is important to the success of your information security and privacy program to maintain metrics. As the old saying goes, “You can’t manage it if you can’t measure it.”

You need to be sure that what you are doing within your information security and privacy program is effective. You need to maintain a number of metrics on an ongoing basis to see where you need to strengthen your initiatives in addition to seeing where you have successes. Not only is this important to you as an information security and privacy leader, metrics are also important to show to your executive leaders to demonstrate the value of your efforts.

Many different metrics can be maintained related to your information security and privacy education efforts. Here are just a few for you to consider:

- **Review question #1.** This question allows the reader to let the CISO/CPO/subscriber know whether or not there have been active social engineering attempts occurring within the business. This also not only raises awareness of the different types of social engineering attempts, but also helps to show the importance of being aware of the actions of those around you, and of the red flags that could indicate social engineering attempts.
- **Review question #2.** This question will reveal how your personnel would react to such a request. This will also show how closely your personnel read the newsletter, and can point out areas where targeted training and additional awareness communications may be needed.
- **Review question #3.** This question will reinforce the reader’s understanding of the topic and show how closely he or she read the articles. It will also provide the CISO/CPO/subscriber information about where more training and awareness may be needed. The answers to this question will also provide metrics for the information security program and the education efforts in particular. You can document how many people responded to the question, and how many answered correctly.
- **Review question #4.** This question will show how well the readers can navigate your company intranet to find information security policy information, or be able to look up policies within printed manuals. The answers to this question will also



provide metrics for the information security program and the education efforts in particular.

- **Website hits**. Track the number of visits to your intranet information security and privacy websites. Take a measurement now, and then track the number of visits immediately following release of “Protecting Information,” and then at least once a week afterwards. See how the numbers fluctuate. When the numbers start trending down it indicates it is time to do another awareness communication, such as a short email blast, a memo, a poster, a scrolling message on the bottom of your intranet website, and so on.
- **Phone calls and emails**. Keep track of the calls and emails you receive in your area, along with the category for the call. Notice how the numbers of calls and emails change after you release “Protecting Information.” Document the categories for the calls.
- **Website logs**. Before releasing “Protecting Information” look at your web site filters. How many social networking websites are blocked? How many on the list are being visited by people on your network? How does this number change after releasing “Protecting Information”?

References for the feature article

There were several facts and examples given within the feature article, “Sweet-Talkers And Alarmists Are Often Criminals.” Here are the references for those facts and examples if you want to know more information about each, or if your personnel ask you for the reference. NOTE: Some news sites will archive their stories after a set period of time and will no longer be available online. If the article is no longer available at a news site you may be able to obtain an archived copy directly from the news organization.

- Page 2: Newark, New Jersey example; Report file with Newark, NJ Police Department, #07-98926
- Page 2: Chicago example; <http://www.dailyherald.com/story/?id=89464&src=143>
- Page 2: Big Five accounting example; http://www.darkreading.com/document.asp?doc_id=140433&WT.svl=tease3_2
- Page 5: Spear fishing information; <http://www.eweek.com/article2/0,1895,2223021,00.asp>

A practitioner’s view

By Anonymous CPO, per his organization’s policies

Unfortunately because of my company’s policies I cannot provide my name or the name of my company. However, wanted to say that the Protecting Information and Awareness Advisor publications have been quite helpful to me, and I wanted to pass along some ideas I’m going to incorporate in case they may help other privacy and/or information security leaders.

I’m planning to:



- Incorporate the definitions from the “Terms You Should Know” into the corporate glossary to ensure the definitions are consistent and can easily be located long after the issue of “Protecting Information” has been released.
- Place archived versions of “Protecting Information” into a central repository that has a link to it from the main Information Security and Privacy intranet site.

With the increased occurrences of social engineering that are documented within news reports, I am very concerned about how vulnerable my company may be to such threats. This issue of Protecting Information discusses social engineering in ways that I know my personnel will understand, and I can build additional training and awareness communications around the information provided.

Let me know what you think!

To meet my goal of making “Protecting Information” as valuable as possible to you, I need to get your feedback. If you can take a few minutes to send me an email at rebeccaherold@rebeccaherold.com and answer the following questions it will help me to determine future topics that are of most importance to the majority of subscribers, along with helping to address your information security and privacy awareness challenges.

1. What part of “Protecting Information” did you find to be the MOST valuable, and why?
2. What part of “Protecting Information” did you find to be the LEAST valuable and why?
3. What topic suggestions do you have for future issues? I want to hit topics that are of the most concern to subscribers, so please let me know. Right now I’m planning to have upcoming issues cover the insider threat, social engineering, and securely working away from the office. However, if I get several subscribers who want a different topic not listed I will change my plans! I want to do what is most valuable to my subscribers.
4. Do you have a child between 10 and 19 that you would like to be considered as a writer for the Youthful View column? I will compensate your child for writing an article; contact me for more information if you are interested.
5. What part of “Your Personal Education Advisor” did you find to be the MOST valuable, and why?
6. What part of “Your Personal Education Advisor” did you find to be the LEAST valuable, and why?
7. Please consider writing a few paragraphs for “A practitioner’s view” within “Awareness Advisor.” If chosen for publication you will receive 50% off your renewal subscription price.

I look forward to hearing from you!

All the best,

Rebecca



Rebecca Herold, CISSP, CIPP, CISM, CISA, FLMI
Rebecca Herold & Associates LLC
1408 Quail Ridge Avenue
Van Meter, Iowa 50261

cell: 515.491.1564

business: 515.996.2199

rebeccaherold@rebeccaherold.com

<http://www.privacyguidance.com>

Blog: <http://www.realtime-itcompliance.com>

Professor at: <http://www3.norwich.edu/msia>

http://www.informationshield.com/privacy_main.html

Author of: The Privacy Papers; Managing an Information Security and Privacy Awareness and Training Program; The Privacy Management Toolkit; The Definitive Guide to Security Inside the Perimeter; The Business Executive Practical Guides to Compliance and Security Risks book series; IT Compliance: The Essentials Series Volume I; IT Compliance: The Essentials Series Volume II; Improving IT Service Support Through ITIL; The Practical Guide to HIPAA Privacy and Security Compliance; Say What You Do; The Encyclopedia of Information Assurance (2008)