SECURITYsense

INFORMATION SECURITY AWARENESS FOR EVERY EMPLOYEE

How to Maximize Your SECURITYsense Subscription: A short user's guide

National Security Institute
165 Main Street, Suite 215
Medway, MA 02053
Tel: 508-533-9099 • Fax 508-507-3631
E-Mail: InfoCtr@nsi.org • Internet: http://nsi.org

I. Security is a Real People Problem

Securing minds, not bits, is the secret to strong information security. Although technologies present incredible opportunities for data, systems and information protection, they can quickly be undermined by uninformed, apathetic, or even malicious employees.

The truth of that statement means that never has security awareness been more important to your company than it is today. You need employees who understand your policies and procedures and are willing to follow them.

In most organizations, achieving that goal is an uphill battle for two key reasons:

1. Employees don't appreciate the critical connection between their behavior, security vulnerability, and the viability of the workplace.

2. Those same employees aren't very motivated to correct point number one.

That's where SECURITYsense comes in, your turnkey solution for tackling the critical human dimension of information security. SECURITYsense cuts through employee apathy and ignorance, and dramatically raises the awareness level of everyone in your company.

II. The Power Behind SECURITYsense

With an effective security awareness program you arm yourself with the ability to incrementally modify the behavior of your employee population, transitioning them from the greatest risk your organization faces to its greatest asset.

An awareness program that works actually brings about a change in the way employees think and act when it comes to security. Your employees' increased understanding and acceptance of strong security practices helps them to see the value of "thinking security," allows them to instantly recognize threats and vulnerabilities, and ensures they take necessary action to mitigate damage.

Three essential ingredients go into creating a security awareness program that works:

1. It must convincingly demonstrate that security breaches don't just adversely affect the organization, but also harm individual employees.

2. It must focus on and consistently reinforce the fundamentals of strong security practice, over and over again in different and creative ways.

3. It must draw people in by appealing to issues important to your employees.

Here’s how SECURITYsense brings real power to your awareness and behavior management efforts:

A Security Problem is Everyone’s Problem

The biggest roadblock to getting your employees to actually change their behavior is their tendency to think of security as “someone else’s problem.” If a security breach occurs, your employees figure, “It may affect the company, but not me really,” or “If I do let in a virus, the IT guys will clean it up with a program or something.”

SECURITYsense helps you knock down that roadblock by consistently hammering home the truth that security lapses do directly affect individual employees. The real stories we present of security disasters dealt to other companies spell out the consequences in detail, so your employees begin to understand companies that suffer losses (financial and otherwise) due to security breaches pass those losses on down the line in the form of layoffs, fewer raises, etc. They also will read about employees who were fired and/or prosecuted as a result of negligence, not following procedure, or even criminal behavior.

The Principle of Repetition

It’s a known fact that repetition assists in the learning (awareness) process. Experts say that a message read or heard several times a day in a given week is virtually memorized and, over a period of a month, 90% of the content is retained. The advertising world knows very well the benefits of repeating a message. Just think for a minute how many times you’ve seen the same ad on TV or in print. Madison Avenue uses the principle of repetition to get its messages burned into the mind of the consumer in order to influence their buying behavior.

Of course your SECURITYsense awareness program won’t reach employees with the same frequency as an ad from Coca Cola, but it does capitalize very effectively on the principle of repetition by exposing them to fundamental “think security” messages every month. We take the critical information security themes, the areas where employees can potentially do the most harm, and reinforce them month after month. Exposure to SECURITYsense means that even your “weakest links” will become stronger over time because everyone is getting the essential messages again and again in new and creative ways.

Bringing Your Security Message “Home”

Experts agree that the key to getting your message heard is to make it relevant to your audience. That’s why so often generic security admonitions fall on deaf ears. Employees passively think of information security as someone else’s job, and therefore not something they need to be concerned about. It is a significant challenge to get employees to take an interest in a topic that seems to have nothing to do with them.

Your SECURITYsense overcomes this challenge in a unique and compelling way by mixing personally relevant security articles with those written from the company perspective. For example, you might find in an issue of SECURITYsense a news article on a hacker who broke into a company database with stolen passwords right next to a story about personal identity theft. Including both types of articles helps you in two important ways.

First, stories of personal security help your employees make the connection to their professional life. As they better understand the information security threats to their own personal and family life, they begin to take seriously the impact of breaches in their workplace. Interspersing these types of personal and family-oriented security articles makes your employees understand that when good security practices are not followed there can be dire consequences, and this newfound perspective motivates them to take seriously the damage that can be done to your company.

Second, these types of stories are perfect “teasers” to get your employees reading and enjoying SECURITYsense. While the rank and file may not be terribly concerned with corporate and information security, they do care about their own security, and the security of their families, homes, posessions and financial well-being. Use the personal security stories to draw them into your total security awareness program. By providing security awareness information for both the home and the workplace you earn credibility with your employees, ensuring they pay more attention to your policy and procedure admonitions.

III. 7 Easy Ways to Deliver SECURITYsense to Your Employees

Communications experts teach that the most effective way to ensure your message reaches everyone in your intended audience is to deliver it through multiple channels. The more opportunities for exposure, the greater the likelihood employees will hear your security awareness message and change their behavior. Here are just seven of the ways you can deliver SECURITYsense in your organization. We recommend you take an approach that incorporates as many of these methods as possible to maximize the power of your SECURITYsense subscription.

Post each new issue on your Intranet’s Web site
Create an amazing online resource for your company by archiving SECURITYsense issues. You can even organize articles by subject for future employee reference, e.g. virus alerts, corporate espionage, social engineering, travel safety, etc.

E-mail the monthly PDF version to all employees
Simply forward the PDF version you receive each month. The contents page comes with bookmarks and links to each security message.

Publish articles in your company newsletter
Send a SECURITYsense article to your organization's internal publisher to reach a whole different group of employees. Be sure to select stories that have the widest range of interest and include the Web address of archived issues.

Make an attractive poster out of any of these quick-read stories
Reach employees even "around the water cooler." Print selected stories on a color printer for posting on bulletin boards, especially in areas where employees don't have ready access to the network.

Create handouts that will actually get read
An excellent tool for illustrating your key points, distribute select stories at formal security briefings to make your briefings more "real" to the employees.

Reprint content for use in memos or bulletins
When you need to make a point or send out a policy reminder, use a SECURITYsense story to help employees understand the reality and importance of your warning.

Create a pop-up window that features an article or tip
Pop-up screens can be positioned to display each time a user logs on to the network, or as a lead to your organization's security Web page, Human Resources page, and other frequently visited locations.

IV. Tips and Techniques to Draw Employees into SECURITYsense

Here's how other SECURITYsense subscribers are spreading the security awareness message and getting employees to respond. Use any of these ideas for yourself, or improve on them and shoot us an e-mail to let us know about it: mail to: SECURITYsense@nsi.org.

Tips for Effective E-mail

- Select a message for e-mailing to all employees once a week (Monday or Tuesday morning works best). Cut and paste one SECURITYsense story, with a link back to the rest of the issue posted on your Intranet. Remember, your goal is to get them interested and in the habit of reading your SECURITYsense! Of the 20 stories you get each month, you'll want to choose the ones that are helpful to your employees personally or center on an issue that is "in the news."

- Use catchy subject lines. The easiest way to do this is simply take the title of the story and paste it in.

- Close the e-mail with a reminder that additional interesting and informative stories on a varitey of topics such as: corporate espionage, travel security, virus alerts, personal security concerns, etc. are available on your Intranet’s security page.

- Provide a link directly to the Contents Page of the current SECURITYsense issue.

Customize Your Message

- You can edit individual SECURITYsense stories and add your own company-specific message. For example, you might take a story on the recent Code Red attack and insert particulars about your organization’s experience with the much publicized worm. Not only do they get an interesting, straightforward explanation of the Code Red worm, but you could add an estimate on the damage done to your company in lost revenues, man-hours, reduced productivity, etc. An explanation of how your existing policies and procedures could have prevented it all (if only they were properly followed) further drives home the point.

Draw Attention to Your Policies

- Instead of putting policy reminders in everyone’s mail box, why not give them an exciting and interesting story about a company/or employee that got burned! Then tack on the corporate policy at the end to drive home your point.

- You can also create links between an individual policy and SECURITYsense stories that help illustrate the need for that policy. When an employee is finished reading a story about stolen passwords costing a company millions of dollars, he or she can easily hit the link to see what your company says about password protection.

Get Other Departments to Spread the SECURITYsense Message

- Anyone in your company can use SECURITYsense stories for internal communication. Leverage the other departments within your company to distribute articles. For example, many of the personal security stories would be well suited for use by Human Resources. Simply let them know your organization has complete rights to utilize SECURITYsense and forward them the issue each month. No matter which articles they choose, be sure they include a link back to the entire issue on your Security Page on the Intranet.

Think about which other departments or individuals might be able to use SECURITYsense articles and let them know about it. Send them this User’s Guide for their reference. You’ll soon find that others in your company are helping get the SECURITYsense message out in ways you haven’t even thought of yet.

- Create links to SECURITYsense issues from other sites on the Intranet, i.e. HR, Legal, Facilities Management, etc.

Advertise

- Put a banner on the company Intranet homepage that links to the current contents page or special articles.

- Publicize the availability of SECURITYsense in the company newsletter, bulletin boards, internal TV monitors, moving message signs, etc.

V. SECURITYsense Brings Awareness, Awareness Brings a Change in Behavior

As a SECURITYsense subscriber you are changing the security culture in your organization. You are ensuring that employees at every level will learn to make the critical connection between their behavior, security vulnerability, and the viability of their workplace by:

- Showing them that a security breach doesn’t only affect the organization, but has a tangible impact on their own professional well-being.

- Consistently reinforcing the fundamentals of strong security practice in new and creative ways.

- Drawing them into your message in the first place through issues already important to them.

Accomplishing these three tasks through SECURITYsense lets you reach your real goal: developing your employees into people who appreciate the risks, put more effort into understanding your procedures, and willingly follow them. In short, you are changing their behavior.

Start maximizing the power or your SECURITYsense subscription today by leveraging some of the tips, techniques and suggestions given in this User’s Guide. In no time you’ll have an employee population armed with the knowledge necessary to defend against a growing array of threats from hackers, spies and information thieves seeking to compromise your organization’s data, systems and proprietry information.