Cyber Security Awareness

Process Methodology for InfoSight Inc's
CYBER SECURITY AWARENESS PROGRAM™

INFOSIGHT
www.InfoSIghtInc.com

Cyber security awareness training is important because no company is immune and everyone makes mistakes.

Contents

Introduction

The Challenge of Security Awareness Training

At InfoSight Inc., we understand that implementing a high-impact cyber security awareness program can be a challenge. A major problem is that annual training (or training on long-term intervals) is really not very effective. Additionally, it takes more than training courses alone to create a “security conscience culture” within any organization. To add to the challenge, the cyber threat landscape is ever increasing, and for it to be effective your security awareness content must adapt in the proper time. Lastly, for maximum effectiveness, testing must occur to identify gaps and adjust to your target audience.

The Impact of Social Engineering Testing

First phish: 30-60% fall victim.

- 6-12 months later: Low as 5%.
- The more often the assessments, the more effective the impact.
  - Quarterly: 19%
  - Every other month: 12%
  - Monthly: 05%
- Over time you will most likely have to increase the difficulty of tests.

As a result of the human factors and the continually evolving threat landscape, our approach to security awareness is holistic and continuous with multiple touch points and levels of engagement.

Effective cyber security awareness initiatives should not be merely training sessions: they should consist of concerted efforts from the top down focused on changing behaviors and encouraging a security-minded culture.

InfoSight's Approach & Methodology

InfoSight Inc. recommends the following process methodology to assist you in building and maintaining your Cyber Security Awareness Program™.

To help you manage your Program, we've divided the it into manageable phases. These phases allow the program team to provide better management and control in order to provide efficient and productive efforts throughout the life of the project. Collectively, these phases provide a dynamic and interactive model for the development of security awareness in the work force.

Phase One
Plan your Program

In the planning phase, you will decide on the ownership, roles and responsibilities of the individuals who will be involved in the program. You will also secure the funding and executive level support needed for a successful program.

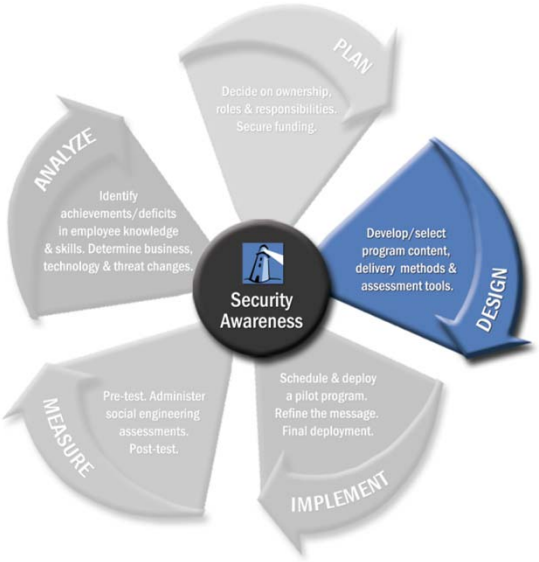
- **Involve upper management**. When upper management says security is important and practices what he/she teaches, people take notice. The same goes for all administrators and managers down the line.
- **Appoint the right person to lead the charge**. Dedicate at least one person to focus 100 percent of their energy on cyber security awareness across the organization. This person needs to be an individual who communicates well and knows how to sell, market, and build relationships.
- **Do your research**. Understand the target audiences and their organizational culture in order to customize your message for greater retention. Different levels of training are likely needed for different job functions.
- **Build relationships.** Security messages must permeate the enterprise for the awareness program to be successful. With minimal resources to carry out the program, it's important to build strong relationships, engage influencers, and nurture those connections.
- **Create ambassadors**. Cyber security ambassadors are the individuals in your organization who are willing to evangelize cyber security awareness and directly influence behavior change.

Determine your budget for the program, including the purchase of cyber security awareness materials such as online learning courses, articles for your website, newsletters, videos, posters, email campaigns, games and other educational content.

Awareness training can ensure personnel have a solid understanding of their employer's security practices and policies. In contrast, one uninformed individual can do substantial harm to an organization's systems and place its data and reputation at risk.

Phase Two
Design & Develop your Program

The design phase consists of developing or purchasing program content, and deciding on the methods you will use to deliver it.



Information security is an important part of doing business today. The message of individual responsibility is critical and must be presented on a regular basis.

Define how you will measure the effectiveness of the program. InfoSight's method of measurement far exceeds traditional standards. Learn more in phase four.

Content may include articles for your website and/or intranet, newsletters, lunch and learns/workshops and webinars, online learning courses, videos, posters, email campaigns, interactive games and on-hold messaging scripts.

Your options include developing your own cyber security awareness materials or purchasing InfoSight's complete education program. Also decide on the types of assessment tools you will use to identify and mitigate deficiencies in your student's knowledge and behavior.

An effective Cyber Security Awareness Program will depend on how well the message is communicated to the audience. Map out a strategy to keep the message in front of your students on a regular basis. Identify where to begin, present the message, reinforce the message, and then build up to the next objective. When mapping out your program, you might want to consider incorporating special dates into the calendar of events.

For example:

- September 8: Computer Virus Awareness Day
- October: Data Privacy Month
- November 30: International Computer Security Day

The Cyber Security Awareness Program is a continuous process and there will be many opportunities to present the security message. Look for ways to embed awareness education into the goals and objectives of each department. Include your message at company events, such as manager's meetings, and utilize email, newsletters and posters to extend your reach. By introducing security awareness materials in a variety of ways, the student is exposed to the topic more than once and will retain the information better.

Phase Three

Implement & Manage your Program

Pilot Deployment, Message Refinement, Final Deployment

To help ensure the overall success of your Cyber Security Awareness Program, you should begin by testing it on a select group of students in a pilot program. This approach allows you to target specific groups with content designed for their level of computer proficiency. Additionally, you might decide to tailor messages for different student audiences based upon their job function, role or department.

The schedule can be based on your student's needs as identified through a risk assessment analysis or it can be based on best practices and standards. Establish a schedule with the most advantageous frequency which will allow you to educate or interact with your students and smooth the path for subsequent communications which will build upon previous lessons. Engage the student with more "touch-points" and make security awareness a continuum with a memorable message.

Content Ideas:

- **Quick-clip Videos** make awareness visual and mobile-friendly.
- **Newsletters** branded for your own security awareness program.
- **Posters & Infographics** to display in an office environment.
- **On-Hold Messaging** to reinforce the message to employees, customer and vendors.
- **Intranet, SharePoint & Internet** content can have themed login messages.
- **Learning Management Systems (LMS)** can be used to track courses.
- **Workshops & Webinars** can be conducted and recorded to be shared later.
- **Interactive Games & Contests** can be used to make it entertaining.
- **Tools** can be provided for download to protect individuals at home, such as malware protection.

Other strategy considerations:

- Rotate key messages as monthly themes throughout the year.
- Choose a new theme for the quarter and build out smaller messages based on the theme.
- Send information security alerts and advisories are used to warn your staff of actual and potential threats to help them keep security awareness top of mind. They can be delivered through e-mail and other traditional channels and should be incorporated into your organization's centralized messaging service when available.
- Incorporate your company policies and procedures as part of your cyber security awareness message.

Phase Four

Measure Program Effectiveness

If organizations take strategic measures to create a training program like that of InfoSight's Cyber Security Awareness Program - and not just throw together a few PowerPoint slides to check training off the "to-do" list - it will better prepare students to help secure corporate systems as well as demonstrate to stakeholders and examiners that your organization is serious about awareness training.

InfoSight also provides a spreadsheet to assist you in measuring the effectiveness of your program. The spreadsheet contains a timeline of activities to help you measure the program's impact on your workforce . It can be used to measure your program's value, including contributions made toward reducing costs and risks.

Testing helps determine how well your "students" have retained the information being taught and to ensure they have a basic understanding of information security. Testing can be performed in a number of ways.

Pre-Testing and Post-Testing

According to an EMA survey, 62 percent consider the completion of training in itself a measurement of training and 55 percent measure its effectiveness by conducting testing upon completion. InfoSight's method of measuring training far exceeds traditional standards. We encourage our customers to survey or test students before implementing the program to determine their baseline of knowledge regarding information security, including the concepts of confidentiality, integrity and availability of sensitive data. Students are surveyed again upon completion of the first 12 months of the program to gauge their resilience towards spear phishing, malware, and drive-by attacks and thus gauge the effectiveness of the Cyber Security Awareness Program. Pre-and-post testing can be accomplished using InfoSight's pre-and-post-program tests/surveys/questionnaires.

Social Engineering Testing

Additionally, InfoSight recommends performing social engineering testing on students throughout the program. In the social engineering assessments, certain students are pre-selected. Simulated phishing attacks are sent via email and phone calls are placed in an attempt to manipulate the student into divulging information that can be used to gain access to more information or assets. InfoSight reports the findings of the social engineering assessments to the customer.

Phase Five
Analyze & Adjust your Program

Metrics and detailed reports are essential to success. They provide continual input for the improvement of the program and related cyber security awareness activities.

Metrics identify gaps where targeted training may be needed. Social engineering reports and course quiz data identify areas of weakness that require attention.

Assess advancements in the threat landscape on a continual basis and adjust content accordingly.

At least annually, review any new additions or modifications to company policies and/or procedures that need to be incorporated or changed within your program.

To reinforce your cyber security awareness effort, decide whether changes need to be made to security technologies in use.

All security awareness programs are unique to each organization. As such, each program takes on a different form and may be carried out in a variety of ways to meet the needs of your organization.

The materials offered by InfoSight Inc. provide a solid foundation upon which the individual program can be tailored, modified and expanded upon and customizations that best suit your business environment can be made.

Officers and directors are under a legal obligation to involve themselves in information security. New federal regulations and state laws impose obligations on all officers and directors to assume an active role in establishing correct governance, management, and a security awareness culture within their organizations.

InfoSight, Inc. offers proven Cyber Security, Risk Management, Regulatory Compliance, and Infrastructure Solutions that protect businesses, financial institutions and their customers from cybercrime and fraud. InfoSight serves enterprise-level business and banks by minimizing risk exposure through security assurance and regulatory compliance. We combine consulting with technology to provide a high level of information security. InfoSight's services include network security monitoring and management, cyber security education, advisory services and regulatory compliance services. For more information, visit InfoSightInc.com, or contact us at 305-828-1003 or info@infosightinc.com

InfoSight's Cyber Security Awareness Program™ is not just another piece of the training puzzle; it's the entire puzzle, and it's ready to use!

InfoSight Inc.
14100 Palmetto Frontage Road, Suite 310
Miami Lakes, FL 33016
305-828-1003 / 877-557-9703