Security Awareness Quick Start Guide

Version 3.0; Last reviewed: June 2017

Handy Hint

If your campus already has an established Information Security Awareness Program and you're able to dedicate more time and resources to developing your own materials, check out the more advanced Security Awareness Detailed Instruction Manual.

Other resources of interest might include the Cybersecurity Awareness Resource Library, the NCSAM Resource Kit, and the year-round Campus Security Awareness Campaign materials.

Quick Start Guide

This guide is for campuses just getting started with a Information Security Awareness Program. It may also serve as a checklist to assess an institution's existing program.

What is an Information Security Awareness Program?

An Information Security Awareness Program is an organized effort to make employees and customers aware of risks to personal and institutional information and information technology, and to provide them with the skills and knowledge necessary to avoid those risks. While the program can be focused on one specific group (e.g., leadership), to be effective in its maturity the program should address all stakeholders, including leadership, employees, customers (i.e., students), and partners (i.e., external service providers). As explained in the CSO article "Seven Elements of a Successful Security Awareness Program," the program should include C-Level support, partnering with key departments, creativity, metrics, 'how-to' information, and multiple methods of delivery.

Why an Information Security Awareness Program?

Community members must understand security and privacy compliance requirements.

- Breaches can have serious legal and financial implications.
- Certain breaches must be investigated and reported promptly.

Community members have a critical role in risk mitigation.

- Attackers are focusing on community members; it is important that they understand the risks to their credentials, and other dangers.
- Community members need to understand how to work with security solutions.

1) Establish an Information Security Program

Without an effective security awareness program, you'll find it difficult to help community members understand the risks they face, the secure methods they should use, and the precautions they should take to keep themselves and others safe. Of course, the first thing to do is get your information security program started. It is important to develop support from senior management for the information security program in order to ensure appropriate human resource allocation and financial support.

2) Develop a Security Awareness Plan

Creating a security awareness plan will help ensure that you have identified your key messages, know who your audiences are, and determine how and when you will communicate with these audiences. Faculty, staff, and students all require different methods of achieving a meaningful level of security awareness. Your IT organization (or information security office) cannot protect your institution alone. The support of the user community is essential.

The materials in this section provide the tools needed to develop your awareness plan and also provide examples of techniques used by other schools. You'll find it helpful to develop a strategy. If you don't, you may find yourself mired in operational issues and may not be able to see any kind of improvement in secure user behavior year after year. But don't forget to "think outside the box" as you develop your plan!

Resources

EDUCAUSE provides a number of resources to help institutions develop and improve their information security programs. While larger institutions may have resources dedicated to information security, many schools may handle information security issues as part of their operational information technology services.

Before getting started, we encourage you to check out the following resources. A few minutes of reading now may save you hours of work later by increasing your chances of getting started down the right path on the first try.

- The Successful Security Awareness Professional: Foundational Skills and Continuing Education Strategies (ECAR Research Bulletin, 2016)
- Security Awareness Plan Template
- Building a Culture of Digital Self-Defense (EDUCAUSE 2017 seminar)
- SANS Security Awareness Annual Report (2017)
- SANS Security Awareness Roadmap
- NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program (identifies the four critical steps in the life cycle of an information security awareness and training program)

Creating a Communications Strategy: Planning Tools

- RIT's 2015-16 Information Security Office Communication Plan

Alert/Advisory Templates (Consider using these templates when preparing e-mail or web portal/intranet communications regarding information security issues.)

- REN-ISAC Alerts and Advisories (2010-present)
- Advisory--Online Scams (RIT 2010)

Integrating Social Networking (Survey community members to learn which social media sites are visited frequently and utilize these communication channels for security messages. To reach students, you must be where the students are (e.g., Facebook, Twitter, Instagram, Tumblr). We've found that many students rely on these sites for up-to-date information.)

- Facebook Fan Pages
  - RIT Information Security
  - UW Information Security
- Twitter
  - Stanford
  - Massachusetts Institute of Technology
  - Brown
  - University of Virginia
- YouTube
  - HEISC YouTube Channel
  - National Cyber Security Alliance Channel

3) Adopt and Modify "Key Messages"

Your audience will only have so much time and patience to hear your messages. Select your messages carefully, present them in an easily digestible format, and try to limit the number of concepts or topics introduced to your audience in each message. Remember, the typical attention span of an audience is 5-10 minutes. If your materials or presentation require more time than that, think about how to break up the content and how to re-ignite audience interest throughout the presentation. Here is a list of sample key messages that are common to most institutions of higher education:

- Unexpected e-mail messages that have you click on links, open attachments, or disclose sensitive information can be seriously malicious…learn about phishing now!
- Passwords that are simple, short, based on dictionary words, or lack upper & lower case letters, numbers, and symbols, are easily guessed by hackers. Change your password now!
- Consider using passwords that are at least fifteen characters, pass phrases, and/or two factor authentication.
- Security is everyone's responsibility. Ask about your role in protecting sensitive information today.
- Information security is a shared interest. Things you do to protect institutional data may very well help to protect your personal information as well.
- Information security breaches are serious, expensive, and can cause life-long impacts on victims.
- Institutions that think they have not been hacked probably just do not know that they have been hacked. Be humble; learn today what you can do to prevent a breach.

After you develop your key messages, back them up with "how to" resources. In other words, do not just tell people to avoid phishing, show them how.

- New Employee Orientation or Faculty/Staff Training
- New Student Orientation
  - Anti Piracy Quiz
  - Security Bookmark placed in student packets
  - Anti-phishing email video
  - Use a Strong Password video

As you develop resources for your program, consult the following resources that address most facets of information security.

- Information Security: Risky Business (*EDUCAUSE Review* article about the top infosec issues campuses are facing in 2017)
- Native Intelligence
- OnGuard Online
- SANS Reading Room
- Online Safety for Higher Education (NCSA)
- Review the Toolkits and Hot Topics pages
- Join the Security Discussion Listserv

4) Establish a Security Awareness Website

Establishing an information security awareness website allows you to communicate effectively and efficiently with members of your institution's community. It can quickly become a trusted resource to:

- provide timely and updated information
- compile external repositories of accurate information for more in-depth reading
- act as your communication hub, promoting additional resources, such as Facebook pages, Twitter profiles, and RSS feeds

If you creating or revamping your program's website, the toolkit Developing Your Campus Information Security Website provides excellent tips, as well as links to other college and university websites. If you're just starting out, don't worry about having to provide authoritative resources for every subject and topic. Leverage the work of other EDUCAUSE peers and that of external organizations, like the National Cyber Security Alliance, and focus on building a comprehensive list of key groups and constituencies on your campus.

Additional ideas for website components:

- What Is Identity Theft? video by the Federal Trade Commission (FTC)
- Cartoons can be linked from your website or shared through social media (e.g., SecurityCartoon.com or xkcd)
- Anti-Phishing Working Group Public Education Initiative
- US-CERT Cyber Security Tips for non-technical users
- MS-ISAC Monthly Cyber Security Tips Newsletter can be published under your institution's brand/logo or linked from your website
- SANS Security Awareness Newsletter, OUCH!

5) Use HEISC Awareness Posters and Videos in Campus Settings

Between 2006 and 2013, the Higher Education Information Security Council (HEISC) hosted an information security awareness video and poster contest. The winning videos and posters—developed *by* college students, *for* college students—are available for colleges and universities to use in campus security awareness campaigns during National Cyber Security Awareness Month in October, student orientations, and throughout the year. Consider using these materials in your campus awareness campaigns whether you print posters for shared student spaces or incorporate the videos into your campus cable channel programming.

- You can access all winning videos on the HEISC YouTube channel.
- You can access all winning posters on the HEISC Facebook page or HEISC Security Awareness Pinterest page.
- Host student video and/or poster contest on your campus. We've developed a handy DIY toolkit for campuses interested in hosting a student content.

6) Publish in Existing Campus Communication Channels

Publishing campus newsletters will allow you to focus on the current security awareness issues that confront your institution. You can also tailor these newsletters to a specific audience (students, faculty, and/or staff) for more targeted campaigns. If your budget allows for printing newsletters, be sure to include an electronic version of each publication on your website, too.

Sample newspapers and articles targeting college and university community members:

- Campus Newspaper (Purdue University)
- Information Security Newsletter (University of Colorado)
- HEISC Monthly Security Awareness Blog Posts (annual Campus Security Awareness Campaign materials)
- IT Newsletter (Stanford University)
- Publishing a security article in a campus newspaper (Carnegie Mellon University)
- Faculty/Staff Newsletters (Purdue University)

Messages can also be delivered at appropriate cycles in the campus newspaper to remind the community of risks such as false claims about expired accounts, IRS e-mail scams, or Valentine's Day viruses. You can take advantage of your IT department's monthly or quarterly newsletter to publish an article on security. Since information security is not limited to the IT department, you can offer to write an article about data classification or data protection in the finance department's newsletter, or in other departments' newsletters. Use your campus television network (if you have one) to run a short security awareness video.

If you have limited resources and cannot create a campus security awareness newsletter, consider sharing the SANS Security Awareness Newsletter, OUCH! This free resource is published monthly in multiple languages, and each edition is carefully researched and developed by subject matter experts. (OUCH! is distributed under the Creative Commons BY-NC-ND 4.9 license, so you may share the newsletter on your campus; the only limitation is that you cannot modify or sell it.)

7) Participate in National Cyber Security Awareness Month (NCSAM)

National Cyber Security Awareness Month (NCSAM), celebrated every October since 2004, was created as a collaborative effort between government and industry to ensure everyone has the resources they need to stay safer and more secure online. Since its inception under leadership from the U.S. Department of Homeland Security and the National Cyber Security Alliance, NCSAM has grown exponentially, reaching consumers, small and medium-sized businesses, corporations, educational institutions, and young people across the nation. There are opportunities for everyone on campus to get involved.

- Conduct community-based security awareness events on campus or regionally.
- Share these tip sheets, which provide in-depth information on how to stay safe in a variety of online settings: on social networking sites, on gaming sites, and on your mobile device.
- Visit the NCSA YouTube channel where you'll find many cybersecurity-related videos.
- Additional awareness resources are also available. Here you'll find other organizations' valuable materials that will prepare you for National Cyber Security Awareness Month.

8) Measure the Effectiveness of your Program Annually

One way of measuring the effectiveness of a security program is by employing the use of an annual user survey. This can be augmented with other types of data that you would collect over time. Consider retaining yearly data for the following:

- User awareness surveys
- Number of incidents, and help desk incident reports
- Computers meeting baseline guidelines

    - Number of machines that have malware protection tools
    - Number of ticket on compromised machines
    - Number of requests for installing and updating malware protection tools
- Number of stolen mobile devices
- Participation at security events
- Awareness quiz scores
- Completion rate of security awareness courses (e.g. PCI, HIPAA, basic security, etc.)

Another way to measure success is to incorporate a “just-in-time” component into your program. For example, with your administration’s permission, launch a non-malicious simulated phishing e-mail to your audience quarterly. Connect those who do not recognize it as phishing and click on links in the message to an educational splash page. Count how many persons were connected to the splash page, and see if over time more recipients recognize these messages as possibly phishing, and fewer click on the links.

Comparing the data over time, one would hope to see better answers on surveys, less incidents, etc.

Other Resources

- ECAR Research Bulletin (2013): Measuring the Effectiveness of Security Awareness Programs
- A Guide to Effective Security Metrics
- Security Metrics EDUCAUSE Resource Page
- Training Evaluation Field Guide (US Office of Personnel Management)
- Evaluating Training Programs (Employment Security Department)
- Delivery Method Matrix (MIT)
- Checklist for Training Process Audit (Scribd)

9) Automate Services

Information Security has the daunting task of staying abreast with the latest threats and zero day outbreaks. Because threats evolve and surface daily, the ability to understand and distribute the information is a challenging task. Information security RSS feeds like the SANS Security Awareness Tip of The Day and US-CERT's Security Alerts make critical breaking news and security tips pertaining to the latest threats immediately available to anyone who subscribes. Leveraging such automated services can reduce workload on information security staff while providing valuable awareness to end users (students, faculty, and staff). You can share these alerts with your community by linking to social media and embedding RSS feeds on your campus website.

Example RSS Security and News Feeds

- Brian Krebs on Security
- Dan Kaminsky on Security
- PC Magazine Security Software
- TrendLabs Security Intelligence Blog
- SANS Institute Security Awareness Tip of the Day
- US-CERT Security Tips
- Anton Chuvakin Personal Blog

RSS Feed Tutorials

- RSS Feed into Twitter and Facebook Tutorial (PDF)
- SANS All about RSS Feeds

Contact a HEISC Awareness & Training Working Group member to help you build your awareness program. The information in this document is only a guide, though it is an excellent starting point!

Top of page
