Security Awareness Program Learning Objectives

By Aron Warren

Last Update 6/29/2012

Module 1: You are a target

Title:

You are a target

Target Audience

Org XXXX IT Staff

Goal

Explain how employees are a target from both domestic and foreign threats.

Background

Government Laboratory employees are a highly valuable target from both domestic and foreign threats. Of the numerous vectors that employees generally encounter in their day-to-day activities we will focus on how employees are attacked through the vector of Internet usage versus in-person contact. Simple email based attacks (tending more toward the spear-fishing) and downloads of software on the Internet are attack vectors to be focused on. This module will supplement the currently required security training materials.

Learning Objectives

1. Highlight several current attack vectors and the associated mitigating behavior. Use the past 6 months of attack vectors having been detected by Cyber Security.
2. Explain how employees can internally determine risk level of their actions while using the Internet. Using the above attack vectors give real world, relatable scenarios, that the employees can identify in their own work days.
3. Name a few of the future attack vectors as given in the June SEC 464 Quarterly Threat Briefing.
4. Explain how current threats to foreign adversaries, eg. Flame, could be adapted to assault US infrastructures, or could backfire causing domestic damage.
5. Re-iterate the key points from the annual required computer security awareness training provided by corporate, tying in points from that training to this module to form cohesion across the trainings.

Module 2: Data protection

Title:

Data protection

Target Audience

Org XXXX IT Staff

Goal

Explain how employees should protect the data of their customers.

Background

Employees should be reminded of the specific ways of how to protect the data of their customers, both unclassified and classified. This information should expand upon then topics discussed in the required annual Data Classification and Security Clearance training but with more detail applicable to the computer based data.

Learning Objectives

1. Protecting unclassified data learning objective will briefly reiterate the different data classifications and categories from the required annual trainings. Once the basis has been restated then moving into how and where that data is used on the networks and servers we administer.
2. After the basics have been covered a transition into the tools available to protect the customer data. Examples of how to move data between our segmented networks will serve as an introduction for new staff members.
3. Classified data protection learning objectives will, again, draw upon the annual required training to restate the basics of data classifications and categories. A reminder will be given that only Need-to-Know people and further specific trainings are required in order to and to have those completed before their due date.
4. After the basics are covered then a brief reminder of who the declassification experts are for our organization as well as what tools are available for the encryption and transport of the various levels of classified data.

Module 3: Encryption

Title:

Encryption

Target Audience

Org XXXX IT Staff

Goal

Explain how encryption can be used in general day-to-day activities

Background

Employees can benefit from an increased use of encryption in their daily lives. This module will offer ideas and areas where encryption might be beneficial such as email encryption during an incident response. This module will expand upon the material presented in the currently required trainings so as to focus on the areas the employees work in.

Learning Objectives

1. List the types of data, both classified and unclassified, that require encryption. This will briefly re-iterate upon the Data Protection module.
2. Where encryption is currently being used that the employees might not be aware of. List the places along the network that data is encrypted but the staff might not be aware of, thusly removing the need for additional encryption.
3. Give examples of where encryption can be used, but is currently not mandatory.

Module 4: Know your Security Operations Center (SOC)

Title:

Know your SOC

Target Audience

Org XXXX IT Staff

Goal

Explain when and how employees can and should engage their SOC.

Background

The SOC performs many duties that benefit both directly and indirectly the employees of org XXXX. This module will explain who the staff currently is, what their duties are and when to engage those employees according to Memorandums of Understanding (MOUs) and additional agreements.

Learning Objectives

1. Introduce Staff, what their names are, what they do, who they report to and what access levels they possess.
2. Explain the SOC's mission, what they do for us, what they monitor, what response times are and what they expect from us.
3. Detail when and how to engage the SOC. This is under what scenarios the SOC is to be engaged. Example being during environmental issues affecting server availability, when a physical security issue has been observed, what to do when after hours work is performed.

Module 5: Data destruction

Title:

Data destruction

Target Audience

Org XXXX IT Staff

Goal

Explain how and when data should destroy data.

Background

Employees are called upon to destroy data on a variety of file system types. This module will explain the tools for achieving data destruction that goes beyond what is provided in the required trainings.

Learning Objectives

1. Unclassified data destruction methods
    a. Staff will be pointed to the current location of unclassified shredders and recycling bins.
    b. For electronic files, the staff will be told about what needs to be done before drives are sent out for destruction.
2. Classified data destruction methods
    a. The staff will be pointed to the current location of classified shredders.
    b. For electronic files, the staff will be told about what needs to be done for proper classified data destruction.

Module 6: Browsing

Title:

Browsing

Target Audience

Org XXXX IT Staff

Goal

Explain how employees can improve their browsing habits.

Background

Employees regularly use the Internet to find answers to questions. Not all employees are aware of tools that make their browsing activities safer for the organization. This module will expound upon practices not included in the required trainings.

Learning Objectives

1. Using browser protection, extensions or add-ons:
    a. NoScript/NotScript for Java protection. MacOSX's latest Java controls.
    b. Updating your Java software from approved software repositories.
    c. HTTPS Everywhere or some similar that prefers HTTPS enable sites.
    d. Flash updating now automatic.
2. Sandboxing your web browser inside of a virtual machine. How to do this and what it buys you.
3. URL Verification is a good way to verify the website you are going to is authentic and (hopefully) malware free. This involved showing the staff how to take a URL and paste it into one of the major security vendor's websites.
4. Employees might be interested in using browsers that automatically update themselves, versus waiting for corporate downloads to be ready.

Module 7: Social Engineering

Title:

Social Engineering

Target Audience

Org XXXX IT Staff

Goal

Explain how employees might be socially engineered.

Background

Employees are pretty isolated and aware of the basic ways of being socially engineered through traditional channels: eg. email, phone calls, etc. This module will go beyond required training to detail how day-to-day conversations with non-employees can be socially engineered to gather information.

Learning Objectives

1. Opportunities outside work for employees to be contacted. Include scenarios from actual employee experiences.
    a. Wearing badges outside of the workplace.
    b. Employees giving out work email addresses, on websites, in mailing lists, on social networking sites.
    c. Patterns of behavior may be learned. What is learned about an employees habits, hobbies, family, traveling may be used against them.
2. Insider Threat
    a. Judging normal requests for information from suspicious requests.
    b. How to report to the security and counterintelligence teams.

Module 8: Mobile Device Security

Title:

Mobile Device Security

Target Audience

Org XXXX IT Staff

Goal

Explain further methods to protect the security of their mobile devices.

Background

Employees who use mobile devices are at a greater risk for data compromise. This module will expound upon the information presented in the current required trainings.

Learning Objectives

1. Laptops connected via VPN and how corporate security can be bypassed by adversaries.
    a. When using the various VPN connection methods, how do each one allow an attacker to pivot through the VPN?
    b. For non-full-VPN connectivity, what are the dangers of allowing others to use that computer? Are there less protections than with full-VPN computers?
    c. Laptops that go on foreign travel services that are available.
2. Mobile phones and how to use the security mechanisms available:
    a. Full device encryption aka. Full disk encryption
    b. Longer than 4 digit password locks for phones
    c. Remote device wiping through Exchange or iCloud
    d. Application Sandboxing and the model that iOS
    e. Knowingly / unknowingly allowing access to your contact list
    f. Applications like XXXX and how their model protects corporate data

Module 9: Protecting your personal computer

Title:

Protecting your personal computer

Target Audience

Org XXXX IT Staff

Goal

Explain how employees should protect the personal computers at home to ensure corporate security.

Background

Employees that use personal devices, eg. home computers, to access corporate resources should be aware of the attack vectors that can be leveraged through their home computers.

Learning Objectives

1. Detail several home computer vectors to gain access to corporate resources such as
   a. Keyloggers
   b. Screen scraping
   c. Leaving VPN sessions unattended
2. Normal suite of antivirus and antimalware
3. Firewalls that are available, either host based or network based:
   a. ZoneAlarm
   b. Astaro Security Gateway
4. Patching, especially automated patching, and various ways of achieving it.

Module 10: Hacked

Title:

Hacked

Target Audience

Org XXXX IT Staff

Goal

Explain how be made aware of current attack vectors through periodic updates.

Background

Employees should be briefed regularly on the current threat vectors.

Learning Objectives

1. Employees are given knowledge of current attack vectors hitting the labs
2. Employees should be reminded, beyond SANS 464 briefings, what signs they should look for to indicate a compromised machine.
3. Employees should be encouraged to seek audits from colleagues to verify security standards are being used, eg. peer audits.
4. What steps should be done if a machine appears to be compromised