Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Methods and Techniques of Implementing a Security Awareness Program

Implementing a successful Security Awareness Program is an essential step in enhancing security within any organization. The mindset and behavior of employees is the crux of the issue - in order to operate at an acceptable level of awareness the organization's employees must have certain basic knowledge to behave 'securely'. What methods and techniques, products and processes can a security awareness program director use to help reach the goal of increasing organizational security awareness? Creating a successful progr...

Copyright SANS Institute
Author Retains Full Rights

AD

William Hubbard
GSEC Practical Assignment, version 1.3
April 8, 2002

# Methods and Techniques of Implementing a Security Awareness Program

Abstract:

Implementing a successful Security Awareness Program is an essential step in enhancing security within any organization. The mindset and behavior of employees is the crux of the issue – in order to operate at an acceptable level of awareness the organization's employees must have certain basic knowledge to behave 'securely'. But how do you, the security awareness program director, provide this knowledge? What methods and techniques, products and processes are at your disposal to help you reach the goal of increasing organizational security awareness?

Some SANS practical papers have indicated what educational tools might be utilized in a security awareness program.[1] Newsletters, tutorials, reminders, mouse pads, and the like all have their place. Yet creating a successful program is not simply a matter of shoving information in the general direction of the user and hoping for the best, it requires the users to learn, understand the significance of, and use the knowledge they obtain. This paper will illustrate why security awareness is so important and what it is supposed to accomplish. Furthermore, it will also cover program contents, methods and techniques of teaching, and resources the security awareness program director might use to better achieve the goal of greater security awareness within an organization. By using the methods and techniques discussed, the program director can develop a dynamic and effective program that both engages employees and helps them learn better security behavior.

In order to understand the importance of security awareness we must first understand that security is about risk management. Any organization has certain information, assets, and products that vary in scope and value. Some are critical to business or government functions, while others are less so. In all cases an organization must protect critical assets, products, and information from theft and misuse or risk losing control of those assets, etc. The organization can protect its assets in many ways. A server, for example, should be physically isolated and protected, have patches applied to the operating systems and applications, have a set of policies detailing how it is to be used and protected, and so on.

By using the Risk = Threat x Vulnerability Model, an organization can determine how at risk the server is (the server, it's information, and it's associated network). If there is a high threat because of Internet connectivity, then the administrator must assess the risk to that server. He can eliminate the risk by disallowing Internet connectivity,

[1] Most of these tools and methods noted are fairly commonplace in an awareness program. Some unique and valuable suggestions have been put forth by Brian Voss, which include the use of social activities such as games, contests, or a Security Awareness Day or Week. (SANS paper: "The Ultimate Defense in Depth: Security Awareness in Your Company"). Also of note is Harbinder Kaur's idea of using a security 'Welcome Letter' for new employees. (SANS paper "Introduction and Education of Information Security Policies to Employees in My Organization.")

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

mitigate the risk by applying patches and locking down the system, or accept the risk with minimal changes. The point is that it is possible to reduce the Risk by reducing the Vulnerability.

The one commonality all organizations share is people. People that create, administer, or otherwise deal with an organization's assets, products, and information. These same people, however, can be a vulnerability to their organization's information and systems. By not using good passwords, locking their workstations, or securing confidential information (the list is a long one…), employees can easily contribute to a system compromise. The less 'security awareness' is present in an organization, the greater the vulnerability is with respect to that organization's people, because if they do not know how to act in a secure manner, they won't. How can we then decrease the Risk inherent in the unknowing masses? Well… we educate them. By teaching employees how to behave in a secure manner, we can greatly reduce 'people-oriented' Vulnerabilities. That is the purpose of security awareness: to give employees the knowledge they need to behave in a secure manner, and by doing so help mitigate Risk to the organization.

It is also important to understand that all employees, to a greater or lesser extent, need security awareness training. In the Armed Forces every soldier, *no matter what they eventually do*, goes through basic training. Similarly, every employee should have security awareness training, because every employee must act in a secure manner for the whole organization to be reasonably safe from 'people-oriented' Vulnerabilities. With regard to the concept of Information Warfare, security awareness is thus part of an organization's Defense-In-Depth. Just as steps are taken to secure assets such as servers, routers, and data, steps must also be taken to ensure secure behavior on the part of the people in the organization. Indeed, the organization's security or even survival may depend on what its employees know and how they act.

What then should a security awareness program do? First, it is important to realize that a security awareness program is a vehicle for the transfer of information. The program director utilizes various means to present this information to the organization's personnel. The information given consists of the organization's security policy, security procedures, and accepted best practices. If your organization has a security policy (or more than one) the security awareness program must reflect and illustrate that policy to have the greatest value to the employees. If your organization hasn't yet drafted a security policy (and it should as soon as possible) then use 'suggested' or industry best practices to instruct on those things that will be included in the future policy. The program material should cover everything you want all employees to know, as they will likely not get viable security awareness instruction from anyone else but you.

Let's look at it this way: 200 years ago did many people know about germ theory? Did they know that they should wash their hands and boil surgical tools to limit the spread of disease and infection? Maybe a few people did, but the vast majority of the population did not. Even though people know these things today, do they always wash their hands before eating, or even after doing something icky? Unfortunately, no, not everyone does, even when they know better. In a way, that's the real challenge – not just to teach people, but also to help them change their behavior. All the security knowledge in the world cannot help people if they don't act on it. (This is your mission, should you choose to accept it…)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

So now you've got a mission, but how do you tell people the message? There are a number of means at your disposal. For example, Patty Hisey, in her SANS paper, provides us with a good road map of what vehicles of communication are available.[2] Indeed their coordinated use can yield a result greater that the sum of their parts. By introducing similar security awareness material in a variety of ways the employee is exposed to the topic more than once and thus will retain information better. The program can utilize both formal and informal methods of instruction. Formal instruction methods include: security awareness tutorials, training courses, testing, formal presentations of security policies, or professional articles in newsletters. Informal methods might include brief newsletter articles, quick notes, lunch meetings, discussion groups, screen savers, posters, and physical reminders like mouse pads, pens, or those neat little tension squeeze balls.

The formal instruction venues usually have more structure and depth to them, and require more time devotion by the employee to master the topic presented. For example, a presentation on new security policies would require the study and understanding of the policy and its ramifications by the employees. These formal presentations, tutorials, or tests need to directly reflect the security policy, for that, in the end, is what the employee is accountable for – following the security policy as it is written.

There are some benefits to more formalized security awareness methods. Presentations usually have the benefit of including time for questions and 'official' answers from the organization's security personnel. You can also reach a great number of people quickly with the same message at the same time. (Efficiency is nice whenever you can manage it.) Tutorials have the benefit of long preparation time, which means less chance for errors in lessons, more involved lessons, and often a combination of visual, audio, and written representations of security awareness information.[3] With this type of formal training you can reasonably expect everyone that takes a tutorial to follow the security tenets covered within it, especially if the tutorial includes testing over the material.

Conversely, the informal methods lend themselves far better to a specific policy or more individualized security themes. A short e-mail note on password requirements, a one-sentence reminder to do the Friday data backup, or a screen saver message that says "Please lock me and keep me safe when you leave" are all examples of this. The message is quick, concise, easily read, and relates directly to one aspect of the security policy. Short reminders or messages are also an excellent way of introducing information that isn't covered in your organization's security policies and procedures or in formalized training. For example, you can create a short article in your newsletter that discusses the specific dangers associated with identity theft. This type of security awareness information might not be in the text of most security policies *per se*, but it can still be beneficial for the employees to know it.

---

[2] Patty lists Posters, Newsletters, Mouse Pads, Pamphlets, Stress Balls, Screen Saver, E-Mails, Daily messages, and Pens. She also notes many useful security awareness topics. (SANS paper: Computer Security Awareness Training… Do You Need It?")

[3] David Sustaita goes into greater detail regarding tutorials, testing, and a good mechanism for testing employees on security awareness. (SANS paper "Security Awareness Training Quiz – Finding the WEAKEST Link!")

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

I have found that people are very willing to take a minute or two to read a quick note – whether it contains new information or simply presents information in a different way than they have already seen. By providing security awareness information in various ways, the audience is more likely to be attentive to each new occurrence than to the same communication type and method every time. For example, you can cover your organization's Internet security policy in a variety of ways to better ensure personnel are aware of the policy and aware of non-policy specific aspects of Internet use.

The official policy referring to Internet use would be in the organization's Operating Security Policy and/or it's Acceptable use policy, and let us assume that some limited use of the Internet is permissible in said organization. You then can publish an article on Internet policy and safe use in your newsletter, send a quick note on some aspect of Internet use (a safe downloading procedure, perhaps), and have a poster illustrating permissible and not permissible Internet use while at work. The non-formal methods (the note, poster, and perhaps the article – depending on how detailed it is) reflect aspects of the written security policy and accepted organizational practices. When the employee reads the short note he or she will read about the particular topic but will also be reminded of the particular security policy it references.

Again, your efforts in security awareness must reflect your written security policy and procedures, and organizationally accepted best practices to have the most benefit for your personnel, and thus your company. If your organization doesn't allow Internet use, for example, you do not need to communicate those issues (unless you are specifically trying to educate people regarding home Internet use). Reference those policies, *et al*, and be sure that they are easily available to company personnel. Placing the information on an Intranet site is an excellent idea, because people can visit the site at their convenience. Try to also archive your other educational materials too, like your newsletters, notes, and best practices, because having easily available educational materials can only benefit your awareness efforts. An internal website can take some time to set up, but in the long run it can serve you and your organization very well as a centralized source for security information. Though providing information is an important part of a security awareness program, it is not enough to make it a truly successful one.

In order for the program specifics to have value they not only need to have useful information (organizational policies, procedures, and best practices), the lessons need to successfully communicate that information to the audience. The crux is to discover how best your audience can learn. No matter what the vehicle of communication is, be it newsletter, note, poster, screen saver, or mouse pad, you must be able to gain your audience's interest and hold it. Also, the lesson has to be acted upon as well as heard and understood. So what methods might you use to 'get everyone's attention' and keep it?

People tend to be easily drawn to pictures and artwork, so why not use them when you can? Illustrate your lessons with diagrams, pictures, figures, and signs. It brings variety into the material so the reader isn't bored with simply reading text. The reader will also have a visual memory as well as a textual reference to draw upon when trying to recall the specifics of an issue.

Themes are also useful, because their use can place the security information into a more familiar context. If the context is more familiar, then the reader will be more comfortable with and interested in the information. They will again be able to draw upon

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the familiar context to recall information about the unfamiliar security issue. To illustrate the value of both illustrations and themes, note the following example of an article I have used in my organization's Security newsletter. It discusses security policy issues and personal use of the Internet.

---

**Safe Web Browsing**

The Internet is rather like a jungle: vast, mysterious, full of useful resources and amazing sights, and it can be a boon for business or personal enjoyment. However, it has its pitfalls, snakes, nasty creatures that want to eat you, and dangerous places that you really want to avoid. Much like traveling in the jungle, one needs to take certain precautions when visiting the Internet.

Make sure your jeep is running well and your travel gear is in good order. That is, make sure your operating system and your web browser have current patches and fixes. If they don't, you may accidentally upload Trojan horse programs, worms, or allow personal information like credit card account numbers to be gathered by nefarious creatures that stalk the Internet. If you use Microsoft Windows and Internet Explorer from home, for example, visit http://windowsupdate.microsoft.com/ at least once a month to stay up-to-date on fixes. Active X, JavaScript, and active scripting features have a variety of security weaknesses and exploits associated with them, so disable them if you don't need them. At work the security settings should have been set by your departmental support staff, so don't change your system or browser configuration. Think of the support staff as your local friendly native guides, they'll help you get safely to the places you want to visit.

Keep your eyes open and watch for potential danger. A firewall can help prevent unauthorized access to your computer and inform you of suspect Internet traffic. Most agencies have firewall protection, but for web browsing from home, a personal firewall is recommended. Free ones such as ZoneAlarm home firewall (at www.zonealarm.com), or

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the Tiny Personal Firewall (at www.tinysoftware.com) are available, or you can purchase products such as Symantec's Norton Personal Firewall (http://www.symantec.com/).

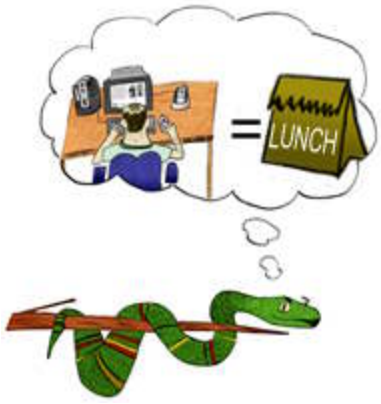
Wear protective clothing and stay inoculated. Use a virus scanner and make sure it's updated. Up to date virus protection will help tremendously in keeping nasty viruses and worms out of your system. (Especially if you access e-mail via the Internet/Intranet.)

Stay on the path. For business purposes, go to the jungle to get what you need, then go home. If your department allows web browsing and you are sightseeing and doing some exploring during a break, be prudent in where you walk. Do not go to known hacker sites, and do not visit sites that your co-workers may find offensive. There are even some sites on the Internet that can attack your system simply by your visiting them – no downloads required. Just like with quicksand, when you realize you're in it, it is usually too late.

Leave the wildlife alone. Do not download anything unless you have the authorization to do so. The Law of the Jungle states: "shareware and freeware from any source shall be installed only with management approval" (from my organization's Operating Security Policy). Even if you are authorized to download from the Internet, it is best not to unless absolutely necessary. If you do have authorization and do download an item, scan it for viruses before opening or running it. Documents, executables, screen savers, videos, patriotic power point slideshows, or anything else – scan it.

Say you've collected a specimen from the Internet jungle. How do you inspect it for nasty things? Well, to scan a downloaded file (in Windows using the McAfee Virus Scanner), right-click on the file and a short menu will usually appear, depending on the type of file. Select 'Scan for viruses' on the pop-up menu. The VirusScan window will appear, and the file you right-clicked on is automatically selected, so you only need to click the 'scan now' button. A second method is to go to the Windows "Start" tab, select Programs, Network Associates, and then select VirusScan. The VirusScan window will appear. You can browse through your drives and choose the file, folder, or drive you want to scan, and then click the 'scan now' button. As always, check with your departmental desktop support staff for the proper procedures for your specific operating system and Virus protection program. (Also of note, some products such as McAfee's VShield can be set up to automatically scan all downloaded files, but again this practice may vary from department to department.)

Anyone can become prey. Please be aware that there are hackers out there that don't care who you are or what you are doing, you are simply a target to them. Like a very hungry carnivore in the jungle, they will eat you if they get the chance. Be mindful that some people are even using the Sept. 11 tragedies and associated issues to lure you to their sites in order to compromise your systems or to get credit card numbers to steal your money.




Remember that many bad things from the Internet jungle are contagious. The 1i0n worm, reputed Chinese hackers, and Russian credit card thieves are all examples of real threats. (Lions and Tigers and Bears, oh my!) If you get infected with a worm or virus, or a bad critter compromises your system, it could dramatically - and badly - affect

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

your agency's network as well. In protecting your own system you are also protecting your agency's network.

Thanks for your time, and be careful – it's a jungle out there.

---

The theme of the note is Internet use and safety (Safe Web Browsing), with reference to security policy and acceptable practices within the organization. The visual theme refers to the jungle, and makes comparisons (similes, actually) to aspects of the jungle to help the reader put the security information into a more familiar or understandable context. Most people will think "Well, I know the jungle can be dangerous, because I've seen Tarzan movies, but how can the Internet be dangerous?" The issues covered in the note refer to the pictures (stay on the path vs. walking into dangerous areas, and there are some not-so-nice people on the Internet), which reinforce the textual messages. The issues within the note actually educate the reader on the Security Policy (with respect to the Internet) and the Acceptable Use Policy as well.

You can revisit this lesson by using the same theme and language in other communication methods as well. Repetition can help people remember, so a poster with an Internet Jungle theme, a best practices Internet checklist on your website, or a pen with the words "Be Careful – It's A Jungle Out There!" can all help people remember the article, and thus reinforce the learning of the security policy and procedures your organization has.

The article "Safe Web Browsing" used above also illustrates the use of humor. Humor can greatly aid your attempts to educate your audience. Would you rather read a bland diatribe on security policy do's and don'ts, or note that makes you smile while it still communicates the same information? If your audience can look forward to your security awareness presentations (in whatever format they may be), they will be far more receptive the message you are trying to communicate. In helping them enjoy the material, or at least the presentation of such, you are helping them to remember it.

Not every message should be couched in witty repartee, however. Just as you should vary the method of communication, you should also occasionally vary the means of communication. When appropriate, use a more serious tone in the message. For example, if there has been a recent security breach in your organization or in one that has similarities to yours, note what can or has happened in a serious tone. Remind the audience of the appropriate security policy and the behavior that is expected of them. I have used an occasional FBI Awareness of National Security Issues and Response (ANSIR) communication to remind personnel to be aware of issues involving terrorism. The effect was sobering, but it also reminded them of how current events might influence the security of the organization.

The use of statistics can also be beneficial, as long as it is not overdone. It should convey one basic idea, but not overwhelm your reader. They are reading your material to become more aware, not for the joy of reading numbers (accountants excepted, of course). Or you can also use statistics to illustrate your organization's successes. For example, you might note how many thousands of Internet attacks have been seen with your organization's Intrusion Detection System in the past month, but be able to say there were no serious system compromises. Whatever your use of statistics is, be sure to tie it

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

into security awareness and acting in a secure manner. The latter is your ultimate goal, the statistic is just a tool to help you help your audience get there.

I have found one of the most successful ways of ensuring that the reader pays attention to a topic is to personalize it. Try to communicate that *they*, not just somebody else, can inadvertently help create a security breach by not using good security behavior. For example, in a security note (A Security Quickie) about e-mail scams and confidential information I conveyed that "The senders want one thing – your money – and will play on your fears, desires, greed, or confusion to get confidential financial or personal information from you", and "In the final consideration, it's only money. **Your** money." By using personalization you can help the reader think about how the issue can affect him or her directly, not just an abstract somebody else. Again, that's really the key, to get each and every person to realize they need to use good security practices to keep themselves, their network, and everyone else connected to it reasonably safe.

Along with choosing what methods and techniques of communication you want to use, you must also decide what resources you want to draw on for the security awareness program. Depending on available money, time, and personnel, you might be able to utilize internal resources or choose to depend on some external resources. Each has certain benefits associated with it.

If you have experienced security personnel within your organization (or willing and experienced non-security personnel), they can be a great boon for the program. By tapping them for articles, topical meetings, and presentations the program benefits from their experience. It also can benefit by their association with the program – if respected organization personnel participate and add to a security awareness program, the program gains some respect simply by their association with it. Another bonus of using in-house personnel for awareness training is that over time trusting relationships can be built around the experienced personnel – trust that can be somewhat transferred to the program, at least in part. Lastly, using in-house personnel for security awareness projects can help build value for those personnel. By performing research, writing articles, and giving security-oriented presentations, they are adding value to not just the program, but to themselves as well.

If your organization performs most of its security awareness training from within the organization, it can build upon whatever experience, knowledge, and educational materials it creates from it. If it has the time and resources available, your organization can even create it's own tutorials, posters, tests, or other educational materials, and in the long run probably cut security awareness training costs.

There are many reasons to outsource security awareness training, too. It is far easier and quicker to utilize the skills of a professional security awareness training company, if speed is of the essence. (Several such companies are noted in the references.) Some companies specialize in particular aspects, such as awareness videos, newsletter creation, posters, or item customization (mouse pads, pens, *et al*). There are also some free sources for security awareness materials, which offer things such as screen savers, security best practices, or other educational materials. (Again, a few of these are referenced below.) The point is that almost any security awareness material you cannot or do not wish to provide in-house can be obtained from a free source or from a security awareness vendor. Each program director must of course decide what is best for his or her program.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

In closing, it is important to always remember the place of security awareness in any organization. It serves an essential role in preparing organization personnel to understand and follow security policies, procedures, and best practices. The security awareness program, not unlike basic training in the Armed Forces, helps make personnel aware of security risks to their organization, whether the risk is from threats of malicious behavior or the vulnerability of ignorance, and furthermore trains them to practice good security behavior.

By varying the methods and techniques of communicating security awareness and good security practices, the program director has a greater probability of promoting security awareness within his or her organization. Along with the variety of methods and means, both internal and external resources can be utilized to benefit a program. The program director must judge what is appropriate and best for their organization, but they must above all keep in mind that it is not enough to simply impart knowledge or awareness. The ultimate goal of any security awareness program must be to change the behavior of the people in the organization.

References

"Companies Aim to Build Security Awareness", Dan Verton, ComputerWorld, November 27, 2000. http://www.computerworld.com/cwi/story/0%2C1199%2CNAV47_STO54375%2C00.html

"Safe Web Browsing", William Hubbard, The Security Blanket, November 2001. Artwork provided by Sam Wong.

SANS Papers:
"Security Awareness: Preventing a Lack in Security Consciousness", Katherine Ludwig, May 25, 2001. http://rr.sans.org/aware/lack.php

"The Ultimate Defense of Depth: Security Awareness in Your Company", Brian D. Voss, August 11, 2001. http://rr.sans.org/aware/ultimate.php

"Introduction and Education of Information Security Policies to Employees in My Organization", Harbinder Kaur, August 29, 2001. http://rr.sans.org/aware/infosec_policies.php

"Security Awareness Training Quiz - Finding the WEAKEST link!", David Sustaita, August 13, 2001. http://rr.sans.org/aware/quiz.php

"Computer Security Awareness Training…Do you need it?", Patty Hisey, December 20, 2000. http://rr.sans.org/securitybasics/training.php

Security Awareness Resources:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Microsoft offers two free security awareness screen savers: the Ten Immutable Laws of Security, and one that displays the Ten Immutable Laws of Security Administration. http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26684

Cybercitizen Awareness Program – probably not too useful for professional organizations, but I include it because it illustrates that security awareness can begin at any age. http://www.cybercitizenship.org/

Vendors:
Commonwealth Films. They have a wide variety of security awareness video and CD-Rom presentations. http://www.commonwealthfilms.com/infosec.htm

Computer Security Institute. This company offers security awareness newsletters, security alerts, and security assessment kits, among other things. https://wow.mfi.com/csi/order/publications.html

Green Idea offers a visual PC presentation/security awareness reminder tool. http://www.greenidea.com/

Interpact, Inc. offers a variety of services including awareness programs, seminars, brochures, artwork, and others. http://www.interpactinc.com/home.html

Native Intelligence, Inc. They offer a variety of awareness services including tutorials, posters, screen savers, animations, and haikus to help educate your personnel. http://www.nativeintelligence.com/

Security Awareness Inc. This company has several offerings including tutorials, posters, screen savers, an awareness workshop, banners, and other educational tools. http://www.securityawareness.com/

Security Web Sites offers a customizable website service, and awareness presentations. http://www.securitywebsites.com/

Sites referenced:

Windows Update: http://windowsupdate.microsoft.com/
Symantec: http://www.symantec.com/
Tiny Personal Firewall: www.tinysoftware.com
Zone Alarm: www.zonealarm.com

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Malaysia @ MCMC 2013 | Cyberjaya, MY | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| SANS Pen Test Berlin 2013 | Berlin, DE | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| Industial Control Systems Security Training - Houston | Houston, TXUS | Jun 10, 2013 - Jun 15, 2013 | Live Event |
| Security Impact of IPv6 Summit 2013 | Washington, DCUS | Jun 14, 2013 - Jun 16, 2013 | Live Event |
| SANSFIRE 2013 | Washington, DCUS | Jun 14, 2013 - Jun 22, 2013 | Live Event |
| SANS Canberra 2013 | Canberra, AU | Jul 01, 2013 - Jul 13, 2013 | Live Event |
| Digital Forensics & Incident Response Summit 2013 | Austin, TXUS | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS London Summer 2013 | London, GB | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS Rocky Mountain 2013 | Denver, COUS | Jul 14, 2013 - Jul 20, 2013 | Live Event |
| SANS Mumbai 2013 | Mumbai, IN | Jul 22, 2013 - Jul 27, 2013 | Live Event |
| SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification | Washington, DCUS | Jul 22, 2013 - Jul 26, 2013 | Live Event |
| SANS San Francisco 2013 | San Francisco, CAUS | Jul 29, 2013 - Aug 03, 2013 | Live Event |
| SANS SEC 560: Network Penetration Testing @ Bangalore 2013 | Bangalore, IN | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| SANS Boston 2013 | Boston, MAUS | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| Critical Security Controls Summit | Washington, DCUS | Aug 12, 2013 - Aug 18, 2013 | Live Event |
| Industrial Control Systems Security Training - DC | Washington, DCUS | Aug 12, 2013 - Aug 16, 2013 | Live Event |
| SANS Thailand 2013 | Bangkok, TH | Aug 19, 2013 - Aug 31, 2013 | Live Event |
| SANS Virginia Beach 2013 | Virginia Beach, VAUS | Aug 19, 2013 - Aug 30, 2013 | Live Event |
| Mobile Device Security Summit 2013 | OnlineCAUS | May 30, 2013 - Jun 06, 2013 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |