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.

Software Piracy- A challenge to E-world

Copyrights, Licensing, Intellectual Property Rights are all terms heard, not understood in a larger part of this global set up. With computers making way to homes in places where the cost of a computer is exceeded by the proprietary software, the resolution of the problem is undertaken by piracy. This paper will be an insight to the levels of the society to which the menace of piracy has rooted itself, the cost and the impact of "illegal" software to the companies. A look at the organizations working to evolve new tech...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Software Piracy- A challenge to E-world

Sundeep Bhasin
GSEC Practical Assignment (Version 1.4b) Option 1
Oct 16, 2002

Abstract

Copyrights, Licensing, Intellectual Property Rights are all terms heard, not understood in a larger part of this global set up. With computers making way to homes in places where the cost of a computer is exceeded by the proprietary software, the resolution of the problem is undertaken by piracy. In these parts of the globe, words like 'free' or 'low cost' are not necessarily associated with low-quality, but on the other hand offers to include millions who otherwise would be simply left out in the cold. Without the aid of these millions of “pirates” some of the “upcoming”, IT outsourcing countries would merely be back to paper bound economies.

This paper will be an insight to the levels of the society to which the menace of piracy has rooted itself, the cost and the impact of “illegal” software to the companies. A look at the organizations working to evolve new technologies that would enhance ways to access and distribute copyrighted works legally, not illegally. The challenges faced by these organizations working with legal issues around the world and the sheer magnitude of the problem. Some of the interesting success stories in pursuing the remedial measures and their cost benefit analysis have also been described.

Software piracy takes toll on global scale

Despite stronger laws and enforcement, software counterfeiting is worsening at an alarming rate around the globe. The lightning growth of the high-tech economy combined with the profit margins in the software industry has led to a feverish global demand for business and consumer software, whether genuine or fake. The cost differentials achievable by software counterfeiting, the ease with which counterfeiting can be accomplished ably aided by Internet growth; it is not difficult to understand the motivation.

Software companies estimate they lost $12 billion in revenue in year 2000 because of counterfeiting. That's 15% of the industry's $80 billion in worldwide sales. The losses experienced by the U. S. dominated software industry will continue to grow as the technology spreads into the Third World economies. With the advent of internet-age into the lesser economies, there is an urgent need to address the anti-piracy measures before providing the trade treaties to facilitate software availability. High-tech and law enforcement experts share a common concern on the need to get a handle over this menace of counterfeiting before

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the problem completely derails the process of software industry growth. There is an urgent need to protect the software industry from becoming an integral part of organized crime operations.

Just a small glance at some of the numbers in the section below would be sufficient to understand the need for a global action team with objectives to contain and control the effects of counterfeiting for the long term future of the software industry.

•**The piracy rate is increasing**. The Business Software Alliance (BSA) reported that the worldwide software piracy rate increased in year 2000 to 37% from 36% in 1999. That means that more than one-third of the software sold worldwide is fake. After a series of strong measures had brought down the piracy rate down from 45% in 1995, the current numbers are a big setback for the efforts of the officials working to crackdown on piracy. The piracy graph had shown a steady decline, until year 2000 upswing changed that trend. The officials attribute the anomaly to the spread of Internet in the Third World countries and a lack of stringent laws to deal with software piracy. In the year 2000, the authorities seized more than $2 billion in fake Microsoft software — a small fraction of all bogus software believed to be on the black market. Another software major estimate that there are more than 5 fake copies for every legal copy. The country with the lowest piracy rate, US, has more that 25% of the software that is not licensed. That speaks volumes about the penetration of software piracy globally. [6], [9]

•**Organized crime is entrenched**. There are growing indications that software piracy operations are being run by not a couple of smart software hackers but it is increasingly becoming a part of organized crime operations. Security experts around the world are conforming the presence of Italian Mafia, Chinese gangs, the Russian Mob, the Middle Eastern terrorists and the Columbian Drug cartels, The modus-operandi is relatively simple, the start of the operation requires a huge investment provided by the gray money of the organized crime. This ensures that the fake software shadows the original software as closely as possible. The increasing availability of software engineers around the globe makes the task only easier. The hackers contribute their part by ensuring that there is no loss of functionalities provided by the software. The distribution of the software is undertaken by smuggling the goods worldwide. With the growth of Internet, even the risk involved in distribution of software has been reduced to a great extent. The lack of laws to deal with piracy means that the penalties associated range from non-existent in some countries to lenient in most others. The profit margins are exponential and it has established itself as a low-risk trade in the echelons of the organized crime sector. [2]

The inability of the governments to deal with these well established and well connected large crime groups is allowing these operations to complement the other nefarious indulgences of the organized crime. The foundation is getting

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

stronger by the day and the losses suffered by the companies and global software economy is rising. The most worrying aspect is that counterfeit rings are growing in number and strength, and some are modeling their operations on the lines of the drug cartels of Latin America. There are strong indications that terrorist elements in Ireland and the Middle East are channeling piracy profits to fund parts of their activities. [3], [11]

•**The growth of the Internet** The risk associated with distribution of the bogus software has been alleviated to a great extent by the spread of Internet to all corners of the globe. Before the Internet, counterfeiters sold bogus software at street markets and other venues. Today, they increasingly peddle their wares on the Web. The criminals utilize the fact that the Internet knows no boundaries and the variable laws in various countries aid and assist them in escaping the legal provisions.

Most of the large software companies have a well-established anti-piracy division, which continuously assess the revenue losses and follows up with legal action against the violators. Microsoft has a search engine that prowls the Internet, seeking pirated software. The company has taken legal action against thousands of Web sites that allegedly offered illegal goods. But cyber-crooks often evade capture. They falsify their e-mail headers and use anonymous post office boxes. They move often, changing their addresses and phone numbers. They utilize the seamless nature of the Internet to their advantage.

However, not everyone can be evasive always. In January, 1999, federal prosecutors convicted two Spanish nationals of selling $1 million in counterfeit software on Software-Inc.com, their Internet business. The two were selling Adobe's Photoshop for merely $99 when the suggested retail price was $995. The landmark judgment resulting in the closure of Napster Inc., a case actively pursued by the music companies, indicates that the awareness of Internet regulations is on a rise.

Looks real: Take a closer look

Thousands of counterfeit manufacturing sites exist in Asia, Latin America and Europe. Some are legitimate businesses that make the illicit software at night. Other sites are hidden in the jungle, protected by armed guards. Investigators have found counterfeit software made in pig farms, shoe warehouses and small grocery stores. A decade ago, small-time crooks made shoddy software in backrooms and back alleys. Law enforcement officers believe that now the world's 50 to 75 major counterfeit software gangs are multimillion-dollar organizations that sell to businesses and governments.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Counterfeiters buy software and copy the entire package, from plastic wrapping to the owner's certificate of authenticity. Computer engineers duplicate the software by reading the computer code and copying it onto a master disk. This is followed by a process similar to legitimate software makers, the counterfeiters use $1 million replicators — huge machines that crank out thousands of software CDs a day. While much of the fake software is bug-ridden, some looks so real and works so well that only experts can tell the difference.

Like drug traffickers, the counterfeiters smuggle their goods in ships, airlines, trains and cars, according to U.S. Customs agents. The crooks will hide bogus CDs in the middle of long spindles, with real CDs on the outside. Or they'll cram illegal software in big ship containers full of toys or clothing. Increasingly, they're sneaking small shipments into the USA in luggage or in Federal Express and DHL packages.

In a case of growing international scope of the problem the U.S custom officials are investigating the case of a Singaporean woman and more than 30 of her U.S. business partners and associates for distributing fake software and laundering the proceeds. She is believed to be one of the biggest importers of Microsoft software. The operations came to light by means of a covert operation where she tried to sell more than $1 million of fake software to an undercover agent.

A Cause for Concern

While software piracy undoubtedly costs manufacturers revenue, some argue the figures are overblown. They claim the statistics are inaccurate because they discount the fact that many people who use pirated software would not have purchased a licensed copy in the first place. The numbers estimating the piracy industry would not be right by just simple multiplying the cost of the fake software with the number of pirated copies sold. The fact is that only a small percentage of people would be able to afford the original software at the legitimate costs. So, piracy is in a way encouraging the users to buy software.

The issues becomes of a prime concern when an aware and educated user admits to have knowledge of the fact that using pirated software is illegal. The issue then becomes even more complex. But, we need to focus on the reasons for educated users to resort to fake software. Most of the users in developing countries would be unable to afford the costs of the licensed software and would not care to purchase it if they didn’t have access to a pirated copy. The software companies have to meet up to the challenge and evolve a more flexible approach to increase penetration of software. [10]

Another challenge for the online distributors is to ensure that the software they intend to retail through Internet cannot be reused for sharing by the users. Most of the users would be unwilling to pay any costs if they are able to get copies of the same software elsewhere for free.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

For many users, especially teens and college students, collecting pirated software has become a compulsive hobby. While no software pirates would comment on the subject many do it for fun. They get a rush and an excitement out of it. They like to pile on the disks with the stuff even though it's not on their computers. It's like a status symbol for the technically aware generation to display their expertise. The idea of free games and songs is attractive but the consequences need to be detailed effectively to desist the tech savvy people from continued indulgence.

Anti-Piracy: Crackdown and Challenges

An effective anti-piracy campaign needs an all out support of the copyright holders, the governments across the globe, the legislation but most importantly it needs a commitment from an average computer user. The owners of the proprietary software should play an active role with the governments to focus of piracy crackdowns. The complex nature of the problem becomes exaggerated because of variable laws in different countries, lack of legislation and implementation. An educated user needs to stand up for the cause of anti-piracy, if there has to be a realistic resolution to this menace.

The Business Software Alliance (BSA) is the foremost organization dedicated to promoting a safe and legal online world. It is the voice of the world's software and Internet industries before governments and with consumers in the international marketplace. BSA members represent the fastest growing industries in the world. BSA educates computer users on software copyrights and cyber security; advocates public policy that fosters innovation and expands trade opportunities; and fights software piracy. Established in 1988, BSA has offices and programs in 65 countries. BSA has been a pioneer in anti-piracy campaigns in various countries. A small account from an incident in Kuwait recently is presented for illustration. [9]

The Hawalli computer district is the scene of action initiated against software pirates by the Business Software Alliance. The pirates erected iron gates to turn the factory into a safe-haven for the "workers" inside. The Police and Ministry of Information officials work with the Fire Department to cut through iron security doors. In the panic of the raid, two members of the gang attempted to jump from first floor windows to try and escape—they don't—the police are waiting for them on the ground. The chaotic scene certainly belies the amount of groundwork that had gone into organizing the raid that began before daybreak. The meticulous planning and the fierce implementation give the impression that it is equivalent to a "war".

It is a war that the BSA is slowly winning, in the Middle East at least. Piracy rates are down from 85% to 57% in 2000 over a period of six years, as a percentage of all installed software The Middle East moved from being the second worst region for piracy in the world to the third as a result in the year 2000. The BSA officials

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

acknowledge the improvements, but believe that the job is only just begun. Illegally copied applications still costs the software industry $240 million in the Middle East alone. The figures are a big motivation for the organization, with the considerable success achieved in last few years the officials are prepared for the arduous task ahead of them. They believe that they can better the expectation and work closely on educating the user as well as the respective governments to make a big difference. [3], [8]

Lebanon, Qatar and Bahrain rank in the top ten of the worst offenders in the world. There are at least six countries in the region figuring in the top twenty worst offenders in the world, which explains the focus attention on the part of BSA. Raids have been directed against both vendors and users of illegal software in almost all territories in the region. The Hawalli raid resulted in over 35,000 CD's of counterfeit software, as well as catalogues and unlicensed software. In Saudi Arabia in November 2000, the authorities emphasized their resolve to work against the menace by running a steamroller over a haul of 300,000 pirate CDs, right in front of computer resellers in the Olaya district of Riyadh. [8]

Winds of Change

Driving the counterfeiters off the street has been a challenge in itself. Setting up a raid requires at least six months of observation, auditing of files and coaxing and cajoling of the target by the BSA, software vendors and other authorities before action is taken. The anti-piracy hotlines, observation and reports from vendors own sales forces are level-one drivers that the BSA works with. The BSA receives thousands of possible cases every year in almost all regions. Thousands of 'soft' warning letters from the BSA are sent, but it is not possible to raid every client. Even after the legal action has been initiated they have had limited success in pursuing these cases. Creating a climate where the authorities are interested in pursuing software piracy has been a task in itself. In many cases the BSA has had to first convince governments to introduce copyright laws to cover software. Then the police and officials need to be trained to identify pirate software, and the judiciary needs to be educated on exactly why software piracy should be taken seriously. Once this is done, it is not always easy to get governments to enforce new laws. Even when action is taken, the courts have taken a while to hand down consistent punishments. [3], [9]

Sentences have ranged from imprisonment and deportation, to very small fines. In every single country of the third world this has been the real problem. The end-user raids have been another problem; since this is issue is very new to these countries. But compared to two years back, majority of these countries are still much better than before. They have more cases, more raids, people are coming to understand the copyright issues. Copyright articles in these countries still need to be amended, but very soon we can expect to see the majority of these countries make amendments especially for Internet piracy and e-commerce.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Progress is being made against counterfeiters, with sales of pirate software being pushed out of all but the smallest retail outlets in many countries, but still some are able to set up operations and begin trading again, as quickly as three months after being raided. To combat this, the BSA has begun concentrating on the end users of pirated software too because they are using counterfeit software or unlicensed copies of legally owned discs. The aim here is not to raid people; it is to get them to legalize their software. Throughout the process of setting up a raid, the target business is given opportunities to remedy illegal software, but too often the excuses are always the same. Businesses claim a lack of understanding of licensing, but this information is available from BSA members, as well as from the resellers, so it is no longer a valid excuse, especially in countries that started implementing copyright law for more than a decade now. The actual response to the raids is effective, if short lived, and aims to be more of a deterrent to others than a preventative measure. The message seems to be strong for a short time; unfortunately it seems to last for a while and then disappears

Pushing this message of education is where the BSA has to focus. The organization works at an international level with governments and official entities, and bodies like the Worldwide Intellectual Property Organization (WIPO) to promote the benefits of legal software. Educational drives include advertising campaigns, working closely with all the related parties and end users. The global initiatives like the recent "Sweeps Week" where BSA offices worldwide worked on highlighting the relevant activities into one week to raise public awareness of their activities, bringing in 159 software settlements, worth $6.2 million. The BSA is partly funded by fines levied in some cases. [5]

The fight against piracy will be a long one. Global piracy rates increased last year for the first time since the study began, and many countries in the West showed no change or an increase in piracy rates, suggesting a deep-rooted core to the problem. The industry faces its biggest challenge from the Internet. Online sites offering pirate software have grown from 840,000 known sites last year to over two million today, and the number is growing. Piracy is already an international business, with counterfeiters moving operations from country to country to stay ahead of local laws, and exporting their merchandise wherever they can.

Anti-piracy measures such as Microsoft Office XP's activation feature are only of limited use—counterfeit copies were available in some cities two months before the official product was launched. The challenge with traditional piracy itself was not a small one but now with the monster of Internet piracy the anti-counterfeiting agencies have to dig deeper into their resources. The laws governing the Internet are still in the evolving stage and their implementation is a different field-play altogether. These sites are based in one country selling software in hundreds of other, the owner with a fake address and a fake number might not even be close enough to pursue. The challenges with the Internet concern not just the anti-piracy organizations like BSA but the businesses, governments, legislators alike.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

We need to nip the core issues in the bud because the Internet revolution is here to stay and unless we firm our resolve to deal with the situation the future of the software industry might be in peril in every single country. [2]

Possible remedies

As a small child we always read that every Technology would be the genesis of some evils but then technology is what needs to redress those evils. The seamless interaction through Internet has brought changes to over lifestyles, to our communication abilities and revolution in our thought process but people have exploited this very mode to pilfer and to violate copyright restrictions. But then we should not let our belief in positive impact of technology dwindle. Some of the stated achievements might appear small in the face of challenge that we have but it is just the beginning. The beginning does of course mean that we are not too far from the solution. Some remedies and their positive impact to the existing scenario are being discussed.

Suggested remedies:

Encourage the use of Open Source Software products
Access to source code will encourage and promote local capacities for software modification and re-distribution. It promotes an environment for technical and systems development, as well as the ability to learn, innovate and invent, while stimulating the local software industry. More importantly it promotes independence from foreign software companies and reduces an outflow of funds from the country.

For instance, a couple of hundred thousand copies of Linux have been distributed across a poor country like India, through local popular computer magazines, at a price of just around $2. That includes both the cost of a slick magazine, and CD. This software with no licensing issues can be legally copied across as many computers as needed. Linux may not be yet ready to replace the proprietary software on desktops but has already penetrated on the back end servers of all the major companies in US. The change is beginning slowly but surely. The e-governance initiatives of various countries in the world are starting to get tied up to the open source software in the market. [4]

The cost alone is not the issue, the idea of openness and sharing opens new horizons in the present software industry. The displacement of the proprietary systems with commodity software and hardware has been resisted in the past due to lack of security and the access times issues. With the growing use of Linux on the back end of the computer networks a sea change is already taking place. The inability to emulate that success on desktops and workstation lies in the lack of adequate technical skills of the end user. Besides, the widespread predominance of 'pirated' versions of proprietary operating systems makes the need for innovation and study of options a low-priority. It is easy to recommend

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

use of Open Source software to save big money and to address the menace of the piracy, but on the ground it takes time to get started.

There have been small but significant ventures around the world especially around the Third World to address the issue of getting people to use the Open Source software. The government officials in Malaysia have been very forthright in adapting to the GNU/Linux initiatives. There has been an earnest attempt to lower the costs of computer software by moving over to Open Source software. The initial costs of setting up and training people has to be viewed as an additional cost but considering the total cost of ownership the Open Source software is making a steady progress into most ventures. The government is promoting Linux in the universities and the schools computer labs on the lines of some top US universities to have abundant and cheap Linux programmers than before. [1]

Securing hardware alongside the software

Software alone can't stop digital piracy; only a totally secured infrastructure has a chance to eliminate the problem. The recommendations come as opposition builds against a proposed bill that would force hardware makers to add anti-copying features to MP3 players and other devices. Although legislators and device makers both see a need for a hardware solution to securing digital content, the groups are at odds over the government's efforts to regulate such technology. Every single device needs to be secured for digital content protection to work according to researchers studying watermarking and security technologies. Some of the content makers are already adding bugs to music and game CDs so that they cannot be directly copied over to unlicensed version. The technology would work against domestic set-ups by teenagers and college students to copy content but to be able to work against the pirate giants a unanimous voice need to be expressed in terms of securing the hardware to contain piracy. [7]

Differentially pricing the software

Some suggest that software should be priced at differential levels, keeping the dollar-earning power of different countries' citizens in mind. Just as books originally published in the US, for instance, are re-published and priced at as little as one-sixth the cost when reprinted in South Asia. This could compensate for the cost differentials that exist in the various parts of the world. Lower costs in these countries would encourage people to buy legal software than otherwise. This could prove to be a big step towards anti-piracy. The utility of this measure would be limited because of spread of software through Internet. However, it will reduce the piracy problems in regions of the world where the problem is at its worst (third world).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Educate the user

The need to spread user awareness is of utmost importance. To educate the user that using pirated software is just like shoplifting. The end user needs to know the impact that piracy causes to the companies and the economy in general would help them realize that it is indeed a grave situation. The government needs to step in the legislation and strict implementation of copyright laws for this to be effective. The government needs to strengthen the legal procedures dealing with piracy and also lend its support for the organizations working against this menace. The copyright laws in every country should become as visible as the laws against theft or shoplifting. The users need to be educated about the fact that the software developers would not invest in a market where their products are pirated which could be a substantial hindrance to the growth of the IT industry in the country. For user awareness, I would request everyone to visit the site http://www.bsa.org [9] to understand the impact and costs involved, the rate of piracy worldwide and the loss to the economies as a result.

Conclusion

The challenge of software piracy is as real and detrimental to the growth of E-globe as the illegal trades are to any society. The path to this battle is long but solutions to a lot of our problems lie within. Every single contribution towards the goal of anti-piracy should be commended. Some beginning has been made and although it appears small today, it might be where the solution ultimately resides. The government of every company is aware of the concerns and the growth rate of E-world would force them to act aggressively on curbing this menace. The government needs to pursue the anti-piracy laws as instruments of state policy. The organizations working towards this goal of anti-piracy should be supported and strengthened to achieve the goal of no-piracy. Every user needs to understand that laws are being enacted every day to curb piracy and if they desire to stay on the right side of the law they should desist from using pirated software. It is only after each and every element of this chain contributes positively that we would head closer to a piracy-free E-world.

References:

1. "Open Source" By Frederic Noronha
   URL: http://www.school.net.th/linux/news/linuxpakistan/

2. "Organized Piracy" By John Geralds.
   URL: http://www.vnunet.com/News/1128619

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. "Crackdown on Piracy" By Mark Sutton
URL: http://www.itp.net/features/print/99370852230521.htm

4. "Resource Poor South-Asians" By Frederic Noronha
URL: http://www.linux-india.org/articles/fred.html

5. "Anti-Piracy" By BSA
URL: http://www.bsa.org/usa/antipiracy/

6. "State Piracy Study" By BSA
URL http://www.bsa.org/resources/2001-11-01.65.pdf

7. "Hardware Key to Piracy" By Robert Lemos
URL: http://computer.org/itpro/homepage/Jan_Feb01/security3.htm
(29 June 2002)

8. "Mideast piracy" from Arabia Online
URL: http://www.arabia.com/tech/article/english/0,11827,47480,00.html

9. URL: http://www.bsa.org

10. "Software Piracy in Singapore"
URL http://asia.cnet.com/sg/0,39002190,10030874,00.htm

11. „Microsoft battles software pirates" By Carolyn Wong
URL: http://www.canoe.ca/CNEWSTechNews0201/15_micro-can.html

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 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