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.

Pockets of Chaos: Management Theory for the Process of Computer Security

The security process is often described as being layered. Some layers are designed to protect, some to detect and others offer fail-safes. The most secure systems are the ones built with security in mind from the ground up. However, more often than not, we are forced to address security as an afterthought. This paper discusses Computer Security as an ongoing journey, not simply a destination and outlines a flexible security framework that manages "pockets of chaos" to better help organizations achieve their security go...

Copyright SANS Institute
Author Retains Full Rights

AD

Streamline IT security environments and compliance processes.

Transforming IT Management.

Jason S. Collins
November 12, 2001
Security Essentials GSEC Practical Version 1.2f (amended August 13, 2001)

"Pockets of Chaos": Management Theory for the Process of Computer Security

Introduction	**2**
The Framework: Security Policy	**3**
Order From Chaos	**5**
The Big Picture	**8**
Conclusion	**9**

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Introduction

Computer Security is something of a dark horse in the information age. In the last few decades, most energy has been directed to realizing the potential of the information revolution to change the world for the positive. There are two sides to every equation though, and we are now faced with addressing the negative manifestations of these societal changes in an environment that was designed to be open not protected. As has often occurred in the past, attention to this matter is being mandated by consequences. Parallels can be draw between the industrial revolution and what has been dubbed the information revolution. The steam engine was a trigger for the start of the industrial revolution much as the personal computer has been the trigger for the information revolution. It was the invention of the railroads though that shrunk the geography of the world and spawned completely new industries during that time. The Industrial Revolution also brought its share of consequences from the destruction of the working family unit to unfair labor practices and ecological destruction. For this cycle the Internet, a global network for the instantaneous distribution of knowledge, products and ideas is the railroads of the twenty first century.[1] This global network has enabled hackers and crackers to commit crimes around the world with little chance of repercussion and given rise to the new phenomenon of identity theft. Computer security was much less complicated in a pre-internet environment. For a computer not connected to the outside world physical access was the major consideration. The advent of the openly connected computing universe in conjunction with the free dissemination of security vulnerability information and tools has created a worst-case situation for protecting our systems. While I am not advocating withholding this information, we have to do something revolutionary in an environment where the people trying to get in know about vulnerabilities as soon as we do. For the information revolution to manifest the scope of changes wrought by the industrial revolution, we the information security professionals must find a way to balance the structure needed for security and dependability with the edge of chaos disorder required to adapt in an ever-changing landscape.

The best most secure systems are the ones built with security in mind from the ground up. What we must work with in reality is security as an afterthought added to a systems built for easy connectivity and little control. The more complex an existing system is the more likely critical gaps will be missed. If for a moment we assumed that we could close all technological holes, there would still be the human element and new holes discovered in the future. People is what the whole system is designed to support, it's reason for being and greatest threat. Though we are forced to address security as an afterthought, it doesn't have to be ad-hoc. Formulating a flexible security framework that manages "pockets of chaos" can help us achieve our goal. Realization that our goal is a self-evaluating process that can evolve as time progresses is the key.[2] The security process is often described as being layered. Some layers are designed to protect, some to detect and others offer fail-safes. Another way of describing the desired security structure is compartmentalized like a honeycomb. Compartmentalization is the idea that not only do you have defense in layers, but more importantly within any given layer there are additional barriers to contain breaches to the smallest area dictated by risk assessment. These compartments are flexible enough to contain the unexpected, or to contain the unexpected within the scope of each compartment. This is the heart of the "pockets of chaos" management theory. Though we are forced to address computer security as an afterthought in today's modern computing

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

environment, if our management of the process is thoughtfully designed and highly flexible we can achieve our goals.

The hardest thing to manage with respect to the "pockets of chaos" philosophy is our own perceptions. For many reasons we chooses to limit our perceptions to a bound "known" space. The bounds of this space are invisible until illuminated by an outside force. When this occurs, some realize their mental boundaries and enlarge the box intact encompassing the new insight while others fight the change by denying is validity or existence. When dealing with the process of computer security, recognition that we can rarely anticipate the unexpected and must be open to continual paradigm shifts is critical. The systems designed from this understanding should be able to accommodate and recognize when the system itself is part of the problem and change accordingly. The only solution is the continued growth and evolution of the process. The implementation of this system is also going to run into the perceptual boxes of the people affected by the change. Fellow employees might view this new system as taking away their rights, or imposing unnecessary restrictions on their actions. In most cases, they are right, a new security process must involve change to the way business is done. It is important to realize that this conflict will occur and address these concerns through an educational program. Taking the time to educate the users to their role in protecting the systems will help smooth the transition and yield better results. Better to have users that don't open e-mail viruses, than trying to limit the damage that can be done. The best password requirements in the world can be defeated by a simple post-it stuck to a monitor. Dealing with the integral human side of the security process can only be ignored at the peril of the project. Addressing these needs during the formulation of the system will yield a much more comprehensive and effective security process.

Several preparatory steps should be addressed prior to getting started. Corporate leadership acknowledgement that a computer security process is needed and beneficial is the first hurdle to overcome. There is often a belief that going out and buying the hottest security tool or hiring a consultant for a vulnerability assessment is all that is needed to be secure[3]. Clarifying what constitutes a secure renewable position is the first step. The next step is the research phase outlining where you are starting from and including a skill assessment of current staff to determine if training/hiring is necessary. Though the computer security field is still young, there are several well-respected security programs. One such program is the CISSP offered by the International Information Systems Security Certification Consortium, Inc[4]. GIAC Security Essentials is another program offered by the SANS Institute[5]. Due to the sensitive nature of the subject, training existing staff might be preferable for their established record of accomplishment and cost savings versus hiring expertise. Individuals establishing and maintaining the security protocols should fall in the highest trust category. Having the right knowledge and skills combined with the correct personnel is essential to ensure that the process being implemented is logically sound and as complete as resources allow. Once management buy-in is achieved, participating staff members have been identified and you have an understanding of where you are starting from it is time to begin.

The Framework: Security Policy

Any serious security implementation must start with appropriate security policies. Michele D. Guel of Cisco's Corporate Information Security Team describes Security Policies as

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

"Providing the virtual glue to hold it all together. Imagine a small city that did not have any rules? What would life be like? The same applies to your organization - policies lay the ground-work."[6] Security Policies are an attempt to quantify a company and it's employee's exposure to risk. For example, an Acceptable Use Policy, which defines that company e-mail is not for personal use, would limit a company's liability if an employee started sending harassing e-mails. It would provide clear consequences for dealing with the employee and shift responsibility for the violations to the user in question. Policies also protect employees in the fulfillment of their duties such as password auditing with a tool like LC3[7]. Without a policy addressing this responsibility, an employee performing an audit under direction from his immediate boss could still be held liable for the activity.

Policy should be developed with or in consideration of a risk assessment for a given liability. Risk assessment is the practice of identifying all possible vulnerabilities to the confidentiality, integrity and availability of data and data systems in conjunction with the consequences of the risk being realized as related to the cost of preventing such a failure. There are several points that are important to realize about risk analysis. The first is that not all risks can be anticipated which is key to the need for flexibility. The second point is the process is about the balance between costs and available resources. No system will ever be 100% secure, and costs rise disproportionately as perfection is approached. A good rule of thumb to apply is the 80/20 rule. You should be able to accomplish 80% of your security goals while only expending 20% of the allocated resources. It can be very beneficial to implement 80% in a first pass, and then use the remaining 20% as a learning exercise in how to enable change management in the system produced. Security Policies will change over time as a reflection of changing threats and needs. The policies both define the security framework and are defined by how the framework manifests over time.

Establishing balanced policies will require participation by representatives from other areas of the company. It cannot be stressed enough that these initial guidelines shouldn't be developed in a vacuum. There is a delicate balance between the level of protection offered and the loss of efficiency due to adherence. By opening the process to appropriate members of the user community a better consensus will be reached and buy-in at all levels will be assisted. Security Policies are rules and as such will likely be meet with resistance. This is why there will have to be a firm commitment to supporting the individual policies as they are defined by the process. If upper management is not fully committed to supporting the individual policies as outlined, they need to be modified until they are acceptable. Policies ignored due to lack of enforcement should not be implemented as they reduce the effectiveness of all other policies. Once Policies are in place they will also need to be updated on at least a yearly basis to re-validate their functionality. Policy review and adjustment should be written into the individual policies for future guidance. Below you will find a short list of security policies which is in part derived from "A Short Primer for Developing Security Policy." by Michele D. Guel[6]:

- Acceptable Use Policy
- Remote Access Policy (where applicable)
- Information Protection Policy
- Perimeter Defense Policy (including external and internal firewalls)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Virus Protection and Prevention Policy
- Password Policy
- Data Backup and Off-Site Storage Policy
- Desktop Management/Configuration Policy
- Server Management/Configuration Policy
- Intrusion Detection Policy
- Audit Policy (can include)
    - Risk Assessment Policy
    - Incident handling Policy

This list is not complete or mandatory, simply a reference for issues that need to be addressed at most companies. Corporate needs, risk assessments and available resources will combine to determine what baseline policies need to be implemented in the initial development. Once a baseline set of policies is established and approved, the next step is converting the policies into a physical implementation.

Order From Chaos

Having established the Who, What, When and Why of what we want to protect, it is time to focus on the how. How do we implement the rules that we have established, confirm whether the guidelines are being followed, detect and determine the source for changes in our environment and know when our security has been breached? The process of security as previously discussed is on-going, constantly evolving through the feedback loop of results. Stephen Norton describes this as the "Circle of Security generally consists of three contiguous and continuous phases: Protection, Detection, and Response."[8] This continuous process is one that is completely driven by and dependent on the flow and processing of data and intelligence. Many times, you will find the word information used interchangeably with data and intelligence, but they are vastly different. Raw data is just a collection of facts letters, numbers, bits, addresses and so on. Intelligence is data that has been analyzed and interpreted as to its cause, effect and meaning. Data is what we collect from each of our security tools and intelligence is what we learn from this data and how we adjust accordingly.

Another critical concept as related to the collection, analysis and response to security information, in a "pockets of chaos" system, is random consistency. If the data is not being pulled and consistently checked, then the process breaks down. This does not mean that the data has to be pulled in or analyzed at the same time in the same way, just consistently. Consistent randomness exemplifies the paradox of the balance we are trying to achieve. If the process becomes rigid and predictable in implementation, it becomes vulnerable to analysis and exploitation. This phenomenon can be explained in a different way using Chaos Theory. Chaos Theory is a new scientific field of study that attempts to deal with seemingly unpredictable systems. Manus J. Donahue III a second year physics student at Duke University defines Chaos Theory as follows:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

> "Chaos theory is the qualitative study of unstable aperiodic behavior in deterministic nonlinear dynamical systems. A dynamical system may be defined to be a simplified model for the time-varying behavior of an actual system, and aperiodic behavior is simply the behavior that occurs when no variable describing the state of the system undergoes a regular repetition of values."[9]

That description is a mouthful. In simpler terms, it means that tiny changes to the starting variables of a nonlinear dynamic system will produce highly varied results and the variables describing the state of the system will not repeat predictably. A visual representation of this is called a fractal. Fractals are mathematical constructs generated by charting the values of variables in a chaotic system. Even though the values do no repeat, there are still patterns evident in the resulting graphs. You may be asking yourself what this has to do with computer security and my answer is I don't know yet. An example of Chaos Theory in computer security would be one workstation out of a thousand that is not patched properly and becomes infected with a virus. This virus could then spread to the entire network through user intervention. The concept of Chaos Theory is already being applied to encryption as a means of generating truly random key information.[10] Chaos Theory is also being applied to the field of artificial neural networks and artificial life.[11] The power of chaotic dynamic systems is that they benefit from the potential at the edge of chaos. The edge of chaos is the transitional area where order and chaos mix yielding new organizational systems capable of dealing with the changing environment.[12] The edge of chaos also yields systems that are bound producing results that fall within a given range over time, yet are unpredictable with respect to exact results. This conceptual idea is what we want to imbue our security process with. At this stage, the application of Chaos Theory to the computers security field is mostly theoretical, but there is much possibility here if it can be recognized.

One approach to implementing a chaotic security system is to capitalize on the strengths of the people and the tools. Computers are good at performing repetitive tasks uniformly and consistently once setup. People are good at providing guidance, insight and the creative spark of randomness that computers cannot yet replicate. We want to spend our energy designing automated processes that are randomized at decision points by input from staff. A system of this nature should exhibit consistency in execution, with a dash of chaos. By spending our energy this way, we maximize our return on investment and leave our staff free to manage the evolution of the process. The first thing that we want to do is to establish baseline snapshots for each of the systems that are to be included in the process. To establish how the process is working over time we have to be able to compare where we are at with where we have come from. These baselines might include:

- Server & workstation security configurations
- Server & workstation port scans
- Server & workstation security logs
- Network foot-printing
- Firewall configurations
- Firewall logs
- Router configurations
- Router logs

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Password vulnerability audits
- ACL audits
- Network User audits
- Backup logs
- IDS Configurations
- IDS logs
- Security Policies
- Antivirus logs

These automated processes can be established and tested obtaining the initial baselines. Additional baselines should be taken periodically replacing the originals. All of the baselines should be stored for long-term comparison in an incorruptible form. Next, we need to update all systems to conform to our security policies using our original baselines to determine what needs to be done. Once we have reconfigured to match our policy configurations and settings, we should take another round of baselines. Then we can set our systems into motion and monitor them over time to ensure that they are performing consistently. One of the best examples of an automated security configuration monitor in a Windows 2000 environment comes from Steve Elky at Software Performance Systems. He provides a step-by-step example of setting up a completely automated system from installation to the collection and parsing of data located at http://www.sans.org/newlook/digests/auto_audit.htm
His system could easily be expanded to include the rest of the auditing required for Windows 2000 boxes. Additionally the methods and tools that he uses could also be adapted to running other tools automatically and collecting the results in a central repository. SANS is host to a wealth of information on free and inexpensive tools and how to automate their use. The reading room is located at http://www.sans.org/infosecFAQ/index.htm and is added to continually by students and members. Defining the mechanics is a topic for many other papers, and I hope that those that read this will pick topics and help fill the gaps.

A very important point about the central repository for security data is that it must be protected with the highest security. With everything gathered in one place, it becomes the ultimate target for a potential intruder. Great care should be exercised in the setup of the repository, who has what rights and when. For the most part there should be no editing permissions on any of the raw data. After the data is collected, it should be stored in a form that it can be used for analysis, but not changed in any way. Baseline data should be stored in an incorruptible form (burned to CD etc) and stored somewhere with very limited access. If the data you are basing your comparisons on can be corrupted then the integrity of the system is lost. With baselines for comparisons and the automated systems brought, on-line the security staff can begin to guide the system and interpret the results. This is where the people involved can contribute randomness to the automated process. Rather than having a list of subnets that are port scanned every night in the same order, someone can select the order or subset to be scanned each day. The time of day that the collection is accomplished can be changed, as well as mixing up downtime for maintenance to the security systems. Staff can also contribute to the effectiveness of the system by creating security issues and the verifying that they are showing up as expected. Spot security breaches by the manager of the process are a great way to audit the security systems and staff. With all of our data being collected and stored securely and our systems in place, we move on to a discussion of interpretation and response.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Big Picture

The final thought on the "pockets of chaos" theory is the big picture. One of the hallmarks of a chaotic system is that state description variables will not repeat values predictably. This does not mean that the state description values are completely random, they simply appear random inside a certain set of bounds. To understand whether the system is functioning we have to look at the system as a whole. When the system is viewed from a big picture perspective patterns should emerge. These patterns are the essence of what we are trying to understand and benefit from. To truly appreciate the system from this perspective we must correlate the data from all of the different systems and tools. This involves selecting criteria of the data from the different systems that can be compared and how it is compared to interpret meaning. This also leads us to think about and treat our systems as a whole. Rather than seeing and treating each subsystem as a complete entity, the big picture lets us work for the health of the whole organization as a living entity. Even though the system is comprised of cables and computers, metal and plastic, it is easily capable of exhibiting behavior reminiscent of life. Another tenant of chaotic systems is that even a simple system comprised of simple components can exhibit unpredictably complex behavior. Today's modern computer and network systems are anything but simple systems of simple components. The most effective tool we have at out disposal to help make sense of all this is the Database.

Databases provide the best organizational structure and tool set to facilitate this kind of data interpretation. Databases, with the data manipulation and control languages that they are built on is the perfect vehicle to help us manage highly complex and rapidly changing systems. Database technology already permeates the security field in antivirus software, intrusion detection systems, vulnerability scanners and all manner of management systems. Databases also play a pivotal role in some of the new industry wide data analysis projects like Dshield.org, which "provides a platform for users of firewalls to share intrusion information."[13] Other projects are striving to provide this kind of initiative at a higher level. The problem many of these initiatives will face is an unwillingness to participate on the part of companies due to the sensitive nature of the information that needs to be shared. This unwillingness to share security and incident information is a major handicap to the security field as a whole. Due to repercussions from stockholders and the market, some companies are unwilling to even report security breaches, much less share information about what they learn. The reasons for these attitudes are understandable, yet they need to be overcome or circumvented. The hackers and script kiddies don't have any problems in sharing their tools and methodologies with each other, why should we.

The database systems designed to help manage "pockets of chaos" needs the benefits of the security industry as a whole. There are security-consulting companies that offer tools under the category of Enterprise Security Management. One tool from Internet Security Systems called RealSecure implements what they call their convergent strategy.[14] Another company, Jerboa Inc. views the process as more holistic.[15] These companies strive to accomplish some of the ideas that have been discussed concerning "pockets of chaos". There is nothing wrong with the goal of making money, but the industry needs an open source solution. The database needs to be

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

modular, where an organization can implement the modules for tools and systems in place and not be burdened with unnecessary complexity. The fundamental rules that drive the database processing are the security policies that we defined in the first step. Security policies are after all business rules for conduct. These business rules should be implemented in the form of analysis rules in comparing the data for compliance. The database also needs to be designed with a mind for extracting the essence of what is learned. This is the process where the security policies are modified over time to deal with new behavior patterns discovered in the process. These rules can then be shared back with the parent organization as a means to overcome a company's unwillingness to directly share security information. The system also needs to be flexible enough to change on the fly resulting from the analysis feed back loop. If a system can be devised that extracts the lessons learned so to speak in a manner that can be returned to circulation without exposing any single organization then we might be able to create a system that is as fluid and dynamic as the one arrayed against us.

Conclusion

Managing Chaos is the ultimate paradox Understanding how to balance the opposing forces of flexibility and consistency is the key to managing the ever-changing security landscape. Computer Security is a journey not a destination. We strive to reach the goal of being secure, knowing that we will not ever succeed. The Information Security Professional is responsible to continually evaluate the security process ensuring the best results possible with the available resources. Just as no security process is complete without user education and involvement, so to should every security staff member have a big picture understanding of the overall goal. For society to embrace the evolutionary possibilities of the Information Revolution, we have to find a way to manage the dangers inherent in this new world order. Protect, Detect and Respond.

Jason Collins

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1. Drucker, Peter. "Beyond The Information Revolution - 99.10." The Atlantic Monthly; October 1999 Volume 284, No 4; 47-57. URL: http://www.theatlantic.com/cgi-bin/o/issues/99oct/9910drucker.htm (03 Dec. 2001).
2. "The Ten Immutable Laws of Security." Microsoft TechNet. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/10imlaws.asp (18 Nov. 2001). Law #10.
3. Oram, Andy. "Cyber-security: Uncle Sam Needs You." WebReview. 26 Nov. 2001. URL: http://www.webreview.com/pi/2001/11_26_01.shtml (03 Dec. 2001).
4. "About CISSP Certification." URL: http://www.isc2.org/cgi/content.cgi?category=19 (14 Nov. 2001).
5. "SANS Training and GIAC Certification Program." URL: http://www.sans.org/giactc.htm (14 Nov. 2001).
6. Guel, Michele. "A Short Primer For Developing Security Policies." 2001. URL: http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf (20 Nov. 2001). Pg 2, 11-28.
7. "About LC3." @Stake Research. URL: http://www.atstake.com/research/lc3/index.html (18 Nov. 2001).
8. Norton, Stephen "Circle of Security" 13 Nov. 2000. URL: http://www.sans.org/infosecFAQ/securitybasics/circle.htm (03 Dec. 2001).
9. Donahue, Manus J. "The Chaos Theory." URL: http://www.duke.edu/~mjd/chaos/chaos.html (17 Nov. 2001).
10. "Secure Information Transmission." 17 Aug. 2001. URL: http://www.rl.af.mil/div/IFB/techtrans/datasheets/encrypt.html (04 Dec. 2001).
11. Gross, Dave. "The Importance of Chaos Theory in the Development of Artificial Neural Systems" URL: http://www.geocities.com/CapeCanaveral/Lab/3765/chaos/neuro1.html (05 Dec. 2001).
12. Petree, Julia. "Part 4: Phase Transition." Chaos Without The Math. URL: http://www.wfu.edu/~petrejh4/PhaseTransition.htm (17 Nov. 2001).
13. URL: http://www.dshield.org/index.html (10 Dec. 2001)
14. "Security Convergence Solutions." (May 2001) URL: http://documents.iss.net/whitepapers/convergence.pdf (22 Nov. 2001)
15. Hale, Robert. Poynter, Ian. Sample, Char. "Holistic Security" URL: http://www.jerboa.com/whitepapers/holisticsecurity.pdf (25 Nov. 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 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**