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.

The Role of IT Security in Sarbanes-Oxley Compliance

The Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act of 2002 requires that the CEOs and CFOs of publicly-held companies certify each annual and quarterly report filed with the Securities and Exchange Commission. This document will summarize the requirements of Sarbanes-Oxley as they apply to IT and define the controls IT must be concerned with in the certification process. This document pertains only to the role of IT and IT security in Sarbanes-Oxley controls compliance; other company depart...

Copyright SANS Institute
Author Retains Full Rights

AD

The Role of IT Security in Sarbanes-Oxley Compliance

Mary Fleming

January 31, 2004

GSEC Practical Assignment

Version 1.4b, option 1

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

1. Abstract 1
2. Introduction 1
3. The Red Tape 2
4. The PCAOB Proposed Auditing Standard 3
5. The COSO Framework and IT Security 4
    - The COSO Report Internal Control Components 4
    - Control Environment 4
    - Risk Assessment 6
    - Control Activities 7
    - Information and Communication 7
    - Monitoring 8
6. Conclusion 8

© SANS Institute 2004, Author retains full rights

1. Abstract

The Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act of 2002 requires that the CEOs and CFOs of publicly-held companies certify each annual and quarterly report filed with the Securities and Exchange Commission.

This document will summarize the requirements of Sarbanes-Oxley as they apply to IT and define the controls IT must be concerned with in the certification process.

This document pertains only to the role of IT and IT security in Sarbanes-Oxley controls compliance; other company departments – accounting, finance, human resources, etc., may be subject to controls not covered herein.

2. Introduction

On December 2, 2001, the day Houston-based energy trading company Enron Corporation filed for bankruptcy protection with $62.8 billion in assets, its stock closed at 72 cents, down from more than $75 less than a year earlier. Many employees lost their life savings and tens of thousands of investors lost billions.[1]

HealthSouth dismissed CIO Kenneth Livesay after he pleaded guilty to federal charges of falsifying financial information and conspiracy to commit wire and securities fraud. Livesay was one of five HealthSouth executives charged by the Department of Justice in connection with a scheme to artificially inflate the health care company's earnings and file false financial statements with the government.[2]

Former Tyco International chairman Dennis Kozlowski and former CFO Mark Swartz are currently on trial for stealing $600 million from the company[3] and "insiders at Tyco are alleged to have received very large personal loans from the company on excessively favorable terms, as well as outright gifts and favors beyond any reasonable measure of fair compensation or furtherance of the corporation's interest."[4]

Criminal activity (alleged shredding of subpoenaed documents, possible insider trading, and knowingly falsifying financial documents) aside, the flaws in the system that allowed [Enron, HealthSouth, Tyco, WorldCom, Adelphia, and others] to hide debt and losses resulted in The Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act of 2002. [5]

---

[1] American Institute of Certified Public Accountants (AICPA) http://www.aicpa.org/info/birdseye02.htm
[2] Apple, http://technologyexecutivesclub.com/SarbanesOxley%20IT%20Role.htm
[3] The Compliance Partners, http://www.thecompliancepartners.com/news.php? news=221
[4] Mays, http://www.eblawsolutions.com/content/ SarbanesOxleyWP.pdf
[5] American Institute of Certified Public Accountants (AICPA) http://www.aicpa.org/info/birdseye02.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Introduced by Senator Paul Sarbanes and Representative Michael Oxley, and signed into law on July 30, 2002, The Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act of 2002 (aka SOX, SOA, or Sarbox), introduced new legislative changes to financial practice and corporate governance regulation: [6] "To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes."[7]

In a nutshell, SOX "requires CEOs and CFOs to certify each annual and quarterly report filed with the Securities and Exchange Commission and imposes criminal penalties for false certifications…And it significantly increases the penalties for security law violations."[8]

What then does The Sarbanes-Oxley Act have to do with IT Security? Buried in the many pages of the new legislation are the requirements that a company's management attest to the effectiveness of "internal controls." Though cited ubiquitously, these internal controls are without definition by the act's authors; they are given their form and function by the internal and external auditors who help a company prepare for and achieve compliance certification. No matter how those auditors define an "internal control," the onus for protecting the financial information and the documents the public relies on for investing rests with the IT department and how they protect the confidentiality, integrity, and availability of that data. While an IT department cannot predict what an auditor may choose to call an "internal control," the basic elements of IT security should be scrutinized and a sound framework of information security should be in place.

According to John De Santis, CEO of Sygate Technologies, Sarbanes-Oxley "is subject to such broad interpretation as to make its implementation and enforcement in the IT world a nightmare."[9] De Santis observes that policy and guidelines must be used to "build a culture around enterprise network integrity"[10] and mechanisms should be implemented to "automate enforcement and remediation."[11]

3. The Red Tape

While Sarbanes-Oxley itself may seem a daunting piece of legalize, auditors will be reliant on additional guidelines as they assist companies in the certification process. IT's roles and responsibilities and their effectiveness in protecting financial information will be analyzed using outside standards mandated by Sabanes Oxley's Section 404.

---

[6] Sarbanes-Oxley Act Forum, http://www.sarbanes-oxley-forum.com/
[7] The Sarbanes-Oxley Act, http://www.law.uc.edu/CCL/SOact/soact.pdf
[8] McCormally, http://www.bakerinfo.com/NR/rdonlyres/e2nu77qp6ecp45tjof v75wi6qscxpal5hyo4eptwpgunaybchlfkh65jwl3tupotj7avlnfiod44ef/Oct02-Sarbanes-Oxley1.pdf.
[9] De Santis, http://www.computerworld.com/securitytopics/ security/story/0,10801,87704,00.html
[10] DeSantis, http://www.computerworld.com/securitytopics/ security/story/0,10801,87704,00.html
[11] De Santis, http://www.computerworld.com/securitytopics/ security/story/0,10801,87704,00.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Central to IT's involvement in The Sarbanes-Oxley Act is Section 404, which "mandates that each annual report contain an internal control report, which must state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. It must also contain an assessment, at the end of the issuer's most recent fiscal year, of the effectiveness of the internal control structure and procedures for financial reporting." [12] In other words, management must assess their own internal controls and an auditor is required to attest to and report on management's assessment.

SOX Section 404 further requires the Public Company Accounting Oversight Board (PCAOB) "to adopt standards for independent auditors to attest to management's report on internal control."[13] PCAOB accepts several frameworks but bases its own documentation on the COSO framework.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has published the "Internal Control — Integrated Framework Executive Summary," a PCAOB accepted guideline for compliance.[14]

4. The PCAOB Proposed Auditing Standard

Its creation mandated by Section 404 of Sarbox, the Public Company Accounting Oversight Board (PCAOB) has written "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements." Herein called The Audit Standard, it "establishes requirements that apply when an auditor is engaged to audit both a company's financial statements and management's assessment of the effectiveness of internal controls over financial reporting. "[15] What the document dictates is how an auditor will review for the purpose of attestation the internal controls surrounding financial reporting.

The Audit Standard charges auditors with two responsibilities: auditing a company's financial statements and attesting to and reporting on management's assessment on the company's internal control. It is this second chore that involves IT and addresses management's assessment of the effectiveness of internal controls. Recognizing that because of inherent limitations (lapses in judgment, human failures, collusion, improper management override) internal controls cannot provide *absolute* assurance, the PCAOB goal for management is an expression of *reasonable* assurance, which "includes the understanding that there is a relatively low risk that material misstatements will not be prevented or detected on a timely basis."[16] Management is required by PCAOB's Audit Standard to "accept responsibility for the effectiveness of the company's internal control over financial reporting, evaluate the effectiveness of the company's

---

[12] Apple, http://technologyexecutivesclub.com/SarbanesOxley%20IT%20Role.htm
[13] Ernst & Young. http://www.ey.com/global/download.nsf/US/Library68/$file/ICGuideMgt.pdf
[14] Ernst & Young. http://www.ey.com/global/download.nsf/US/Library68/$file/ICGuideMgt.pdf
[15] PCAOB, p. A-7
[16] PCAOB, p. A-12

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

internal control over financial reporting using suitable control criteria, support its evaluation with sufficient evidence, including documentation, and present a written assessment about the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year."[17]

As The Audit Standard also charges auditors to "evaluate all controls specifically intended to address the risks of fraud,"[18] management has the responsibility to "design and implement programs and controls to prevent, deter, and detect fraud."[19]

5. The COSO Framework and IT Security

The PCAOB Auditing Standard requires that management "base its assessment of the effectiveness of the company's internal controls over financial reporting on a suitable, recognized control framework established by a body of experts."[20] Any framework that meets PCAOB's standards is acceptable for use, but "the performance and reporting directions in [The Audit Standard] are based on the COSO framework, "[21] i.e., "Internal Control — Integrated Framework Executive Summary" written by The Committee of Sponsoring Organizations of the Treadway Commission (COSO). So that auditors may apply the PCAOB standards in a reasonable manner, PCAOB requires that any framework used should encompass all the themes covered by the COSO Internal Control Framework, herein called The COSO Report.

The COSO Report (or any other approved framework) will be used by auditors to assess more than just an IT department, but our focus will be on how The COSO Report can be used by IT managers to prepare for the audit.

The COSO Report Internal Control Components

COSO describes Internal Controls as consisting of five inter-related components: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring.[22]

Control Environment

The Control Environment is the philosophical foundation of a company and its attitude toward information security. (RW) Control Environment points of focus are: integrity and ethical values; commitment to competence; board of directors or audit committee; management's philosophy and operating style; organizational

[17] PCAOB, p. A-13,14
[18] PCAOB, p.A-15
[19] PCAOB, p. A-15
[20] PCAOB, p. A-10
[21] PCAOB, p. A-11
[22] COSO, http://www.coso.orgO

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

structure; assignment of authority and responsibility, human resource policies and procedures.[23]

Integrity and Ethical Values

This point of focus will expect that the company's policies – in this limited case, especially information security policies – are embraced at the top of the organization. The buy-in and support of C-level management of the development, implementation, and enforcement of strong information security policies and best practices are instrumental in establishing a compliant control environment.

Commitment to Competence

While job descriptions may be the purview of Human Resources, auditors will be ensuring that IT assures that personnel possess the knowledge and skills needed to perform IT jobs adequately.

Board of Directors or Audit Committee

In addition to participating in larger, company-wide organizations comprised of several departments, IT may have its own groups committed to policy development, implementation, and enforcement; researching information security issues (wireless, remote access, exception reviews); or manning disaster recovery and business continuity teams.

Management's Philosophy and Operating Style

Geared toward the financially side of the house, this point of focus can be impacted by how IT security reacts to risk assessments and how liberal or conservative information security policies are.[24]

Organizational Structure

IT's position in the organization's structure and how "its ability to provide the necessary information flow"[25] will be scrutinized as will be the "adequacy of knowledge and experience of key managers." IT should have information, system, and network security roles and responsibilities defined and documented.

Assignment of Authority and Responsibility

Documented with roles and responsibilities should be the delegation of any IT duties, IT employee job descriptions, skill level requisites, standards and procedures. [26]

---

[23] COSO, http://www.coso.org
[24] COSO, Internal Controls – Integrated Framework, p. 32
[25] COSO, Internal Controls – Integrated Framework, p. 32
[26] COSO, Internal Controls – Integrated Framework, p. 32

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Human Resource Policies and Procedures

While this point of focus is obviously not overtly an IT issue, IT should be aware of HR policies as they relate to information security – appropriate background checks in hiring, security awareness training, remedial action for security policy breaches.[27]

Risk Assessment

According to The COSO Report, "risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change."[28]

A precursor to many information security activities, Risk Assessment is an examination of the company's vulnerabilities and the threats to its security.

As described by Eric Maiwald, author of Network Security: A Beginner's Guide, a risk assessment "is used to determine the value of the information assets of an organization, the size of the threats to and vulnerabilities of that information, and the importance of the overall risk to the organization." A risk assessment of the financial information assets is critical to "effectively implement a proper security program"[29] and thereby to the compliance with Sarbanes-Oxley and SEC requirements.

Risk Assessment points of focus are: entity-wide objectives; activity-level objectives; risks; and managing change.

Entity-Wide Objectives

IT and information security obviously will play a supporting role in this point of focus. The requisite departmental plans and budgets compel IT to be actively involved.[30]

Activity-Level Objectives

At the Activity level, IT objective-level plans expand "as goals with specific targets and deadlines."[31] Ongoing review of information security controls, keeping policies current, implementing countermeasures to new threats, security awareness training, specific security-oriented projects, may be considered activity-level objectives.

Risks

Risk will be assessed at the entity (company) level and the activity (departmental) level and specifically, information systems. A risk assessment

---

[27] COSO, Internal Controls – Integrated Framework, p. 32
[28] COSO, http://www.coso.org
[29] Maiwald, p.95
[30] COSO, Internal Controls – Integrated Framework, p. 47
[31] COSO, Internal Control – Integrated framework, p. 153.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

of IT, including internal and external factors, can identify the threats to overall and financial information and address IT's responsibility to countering them. IT should have in place the automated "mechanisms to identify risks arising from external …[and] internal sources."[32]

Managing Change

How IT stays abreast of or even ahead of the ever-evolving threats will be scrutinized in light of how those threats affect the security of a company's financial information assets. New technology changes can be either legitimate or illicit, and how IT responds to those changes will be under review.

Control Activities

COSO defines control activities as "the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliation, reviews of operating performance, security of assets and segregation of duties."[33] COSO divides control activities into three categories, operations, financial, and compliance. IT activities such as policies, awareness training, log reviews, inventory, segregation of duties, physical security, electronic access to data, files and programs, change control procedures, may fall into one or more categories.

COSO indicates two categories of controls over Information Systems – general and application controls. General controls "include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance."[34] These same controls may have been addressed in the IT department reliant on ISO 17799 as an information security guideline. Application controls are those governing the "completeness and accuracy of transaction processing, authorization and validity."[35] The requirements that security be built in to applications in development results in the application controls of edit checks on "format, existence, reasonableness"[36]

Information and Communication

Information is the core of a business, and assurance of the reliability of financial information is the basis of The Sarbanes-Oxley Act. A key responsibility of IT is to safeguard information, financial and otherwise, internal and external. As the custodian of a business's information, IT's analysis for the COSO report should include reporting on the mechanisms in place "for identifying emerging

---

[32] COSO, Internal Control – Integrated framework, p. 47.
[33] COSO, http://www.coso.org
[34] COSO, Internal Control – Integrated framework, p. 52.
[35] COSO, Internal Control – Integrated framework, p. 54.
[36] COSO, Internal Control – Integrated framework, p. 54.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

information needs…information needs and priorities are determined…and a long-range information technology plan has been developed and linked with strategic initiatives."[37]

The COSO Framework also measures communication, and while not singularly an IT function, IT information security policies, awareness training, and ongoing education concerning security vulnerabilities should not be discounted as elements for COSO consideration. The sensitivity of information should be addressed in policy as well as how information is transmitted. In support of the point of focus communication, network connectivity, access control, and encryption may be cited as internal controls.

Monitoring

The process of monitoring internal control systems "that assesses the quality of the system's performance over time… is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two."[38]

Ongoing monitoring is the day-to-day scrutiny of operations and activities and "includes regular management and supervisory activities, and other actions personnel take in performing their duties."[39] Monitoring as a point of focus may entail network traffic monitoring, the logging and review of intruder detection systems, or just ensuring that systems are operational.

Separate evaluations are derived from the ongoing monitoring and the assessment of risks and the effectiveness resulting from them.[40] Monitoring may highlight an area where more intense scrutiny is warranted (incidents of external or internal intrusion; or an internal exposure to a virus, worm, or Trojan.)

6. Conclusion

While Sarbanes-Oxley is financial legislation, IT plays a strategic role. According to Ben Apple, "since IT systems are used to generate, change, house and transport that data, CIOs have to build the controls that ensure the information stands up to audit scrutiny. It's inevitable that CIOs will also be held liable for invalid data." [41]

Meeting Sarbanes-Oxley requirements will be strongly dependent on a company's IT security program. "Ensuring appropriate awareness of company security policies and commitment by management; designing and implementing appropriate security controls; and documenting and auditing security policies,

---

[37] COSO, Internal Control – Integrated Framework, Evaluation Tools, p. 170.
[38] COSO, Internal Control – Integrated Framework, p. 69.
[39] COSO, Internal Control – Integrated Framework, p. 69.
[40] COSO, Internal Control – Integrated Framework, p. 71.
[41] Apple, http://technologyexecutivesclub.com/SarbanesOxley%20IT%20Role.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

and making sure they are understood by management and end users,"[42] are among the Act's requirements.

While Sarbanes-Oxley is primarily a concern of financial departments, IT has an important supporting role when the audit and compliance theatrics begin.

For those public companies who do not currently have in place adequate information security policies, practices, and procedures, Sarbanes-Oxley may be the impetus to implement such. For those companies who already live by policy, Sarbanes-Oxley and the attendant audits will compel them to remain current.

© SANS Institute 2004, Author retains full rights

[42] Apple, http://technologyexecutivesclub.com/SarbanesOxley%20IT%20Role.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

1. American Institute of Certified Public Accountants (AICPA) "A Bird's Eye View of the Enron Debacle." URL: http://www.aicpa.org/info/birdseye02.htm.

2. Apple, Ben. "Sarbanes-Oxley Act: The IT Department Role. " URL: http://technologyexecutivesclub.com/SarbanesOxley%20IT%20Role.htm.

3. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Internal Control – Integrated Framework. American Institute of Certified Public Accountants. July 1994.

4. Committee of Sponsoring Organizations of the Treadway Commission (COSO). Internal Control – Integrated Framework; Evaluation Tools. American Institute of Certified Public Accountants. September 1992.

5. De Santis , John, "Why network security should go further than Sarbanes-Oxley." December 4, 2003. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,87704,00.html

6. Ernst & Young. "Preparing for Internal Control Reporting." URL: http://www.ey.com/global/download.nsf/US/Library68/$file/ICGuideMgt.pdf

7. Maiwald, Eric. Network Security: A Beginner's Guide. New York: Osborne/McGraw Hill, 2001. 400.

8. Mays, Bill. What Do Recent Corporate Scandals and the Sarbanes Oxley Legislation Mean for the Directors and Officers of Privaately Held Companies? October 2002. URL: http://www.eblawsolutions.com/content/SarbanesOxleyWP.pdf

9. McCormally, Timothy J. "Of Newton, Heisenberg, and Sarbanes-Oxley – Corporate Accountability and the Provision of Tax Services." URL:http://www.bakerinfo.com/NR/rdonlyres/e2nu77qp6ecp45tjofv75wi6qscxpal5hyo4eptwpgunaybchlfkh65jwl3tupotj7avlnfiod44ef/Oct02-Sarbanes-Oxley1.pdf.

10. Mogull, Rich, Debra Logan, and Lane Leskela. "CIO Alert: How You Should Prepare for Sarbanes-Oxley." URL: http://www4.gartner.com/resources/117600/117627/117627.pdf. October 1, 2003.

11. One Hundred Seventh Congress of the United States of America. "The Sarbanes-Oxley Act of 2002." URL: http://www.law.uc.edu/CCL/SOact/soact.pdf

12. Public Company Accounting Oversight Board. "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements." October 7, 2003. http://www.pcaobus.org/rules/Release2003-017.pdf.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

13. Sarbanes-Oxley Act Forum. URL: http://www.sarbanes-oxley-forum.com/index.php.

14. Securities and Exchange Commission. "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports." June 11, 2003.

15. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). "Internal Control - Integrated Framework Executive Summary." URL: http://www.coso.org.

16. The Compliance Partners. Sarbanes-Oxley News & Developments, Good Governance Begins At Home. December 15, 2003. URL: http://www.thecompliancepartners.com/news.php? news=221

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 19th, 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**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**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**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**