Global Information Assurance Certification Paper

Deborah S. Weinstein
GIAC SEC 1.4

Outsourcing and Off Shoring Security Concerns
Or, What I Wish I Knew Before My First Outsourcing

Abstract

In today's tough economy, more companies are outsourcing and/or off-shoring activities that were traditionally performed in-house. Information Technology (IT) and desktop support, call center management, security and network administration[1] are now commonly outsourced as a cost cutting measure. Ideally, a seamless transition of personnel and applications to the outsourced company is achieved while the levels of security, system access requirements, and system features and functionality are maintained or even improved. Not accounted for in the balance sheet benefits may be concealed a new drain on resources. Additional security vulnerabilities are often introduced and the cost to mitigate these vulnerabilities is often not identified or funded[2].

In addition to outsourcing work, many companies are off-shoring work to countries where the labor rates are cheaper. A recent study by the *Garner Group* predicts that by 2004, more than 80% of U.S. companies will consider off shoring critical IT services, including software development, to countries such as India, Pakistan, Russia and China.[3] Balancing the economic benefits, off shoring presents a variety of challenges. Terrorist groups may target international operations and for that matter, a single rogue programmer can add malicious code to t software that is developed for off shoring companies[4]. It is difficult, and often impossible to validate that the software that is developed offshore does not contain bugs, worms, or back doors. Additional complexity is added to the development of systems and the administration of devices because of diverse political situations[5], different telecommunication laws, country specific encryption standards, and diverse written and spoken languages different from those in Western Europe and North America.

Introduction

Outsourcing and off shoring have blurred network boundaries, as they entail greater network access for contractor employees to key internal components, including administrative permissions and responsibilities. This shift in the management of applications, servers, and networks has required the re-architecture and/or redevelopment of applications and access methodologies in order to maintain the pre-contract levels of security. Changes in the administration of desktops and servers have increased the number of remote

access software packages allowed through company boundaries. Such arrangements heighten system vulnerability.

There are many instances when outsourcing a single function such as Intrusion Detection System (IDS) deployment[6], anti-virus deployment[7], or performing network and system back ups[8] can be deployed with reduced costs while maintaining the security of the enterprise. In these cases, it may be possible to segregate applications and networks, deploy Demilitarized Zones (DMZs) to transfer information between companies, and only permit access to a small portion of the corporate infrastructure. This paper, however, will address the difficult situations when the network is not well defined, key applications are shared or cannot be made standalone, or a majority of infrastructure resources are required to maintain or use applications such as DNS or Microsoft domain/WINS resources such as desktop support management.

In order to ensure the outsourcing does not compromise security and/or off-shoring contract, the outsourcer's Security Organization must be an integral member of the contract and execution steering committee.[1] The Security Organization must participate in all phases of contract negotiation, implementation, contract life and termination. A feasibility study should be performed prior to any contract negotiations to address unique security and implementation issues associated with the potential work. The cost of the negotiated efforts increases greatly if studies are not done prior to contract negotiation because elements are missed or additional work is required to maintain or increase the current level of security. If the study is to be performed jointly by the outsourcer and outsourcee, the outsourcer should sing a non-disclosure agreement to prevent this information being released prior to the actual contract finalization.

The Security Organization must ensure that the new architecture, work model, and contract-specific implemented safeguards do not remove pre-existing security safeguards. The Security Organization must also ensure that the contract safeguards are indeed implemented during the life of the contract to compensate for additional vulnerabilities created during the outsourcing and/or off-shoring process. Periodic reviews of the contract must also be done to identify contract scope creep, new applications or added technologies, and changes in locations or personnel.

This paper will define steps that should be taken at the contract negotiation, implementation, during the life of the contract, and at the contract termination. Before proceeding, it should be noted that each outsource/off-shoring contract is unique and all identified issues may not be applicable in all cases.

[1] For the purposes of this paper, the outsourcer is the company contracting the outsource/off-shoring activities, and the outsourcee is the company that will be performing the services.

The majority of issues will surface during the contract negotiation and implementation phases. The implementation phase will flush out any needed security modifications and process improvements. In addition, this is the phase where the majority of personnel issues arise, and access to systems need to be modified. Many applications and systems will require development work to restore levels of security previously available due to the change in personnel. The costs for this effort must be included in any business case or model.

Contract Negotiation and Feasibility Studies Issues

Prior to any discussions with an outsourcee, non-disclosure agreements must be in place. These agreements will protect outsourcer proprietary information, especially if the negotiations cannot be completed. It is important that a security review be completed on the affected systems, applications, and network prior to contract finalization to identify any gaps in the outsourcer's security policy or to mitigate risks caused by the new access. If a feasibility study is performed, the security reviews should be completed then. Network assessments, network sweeps, application scanning, review of security logs and security auditing software results, and review of access (protocol) and authentication requirements will provide a baseline from which security gaps and safeguards can be addressed.

In order to ensure a successful outsourcing and/or off-shoring, a working framework must be agreed upon, particularly in the areas of security policy and implementation, software and hardware standards and licenses, quality metrics and service level agreements including dispute resolution[9], personnel issues, and identification of where the work will be performed. In addition, specific security products and customer specific implementation issues must be identified. Anticipating these issues during negotiations will ensure clear definition of roles and responsibilities, establish points of contact for security questions and interpretation, and develop a mediation channel to resolve issues.

The security policy settled on during negotiation must be provided to all parties, and, furthermore, there must be an agreement on security update policy guidelines. Additional policies that increase the overall security may be added to the contract for incorporation during the implementation and life cycle phases of the project. All subsequent security judgments and recommendations, however, must proceed from the standards laid out in the guidelines. Authorized security policy interpretation should be entrusted to a policy steering committee made up of representatives from both company's security organizations. Outsourcer and outsourcee steering committees should also be established, moreover, to resolve day-to-day security issues arising out of the contract. Contract language must spell out a negotiated timeframe for implementation of all security policy changes.

In developing the contract, it is essential that the affected users groups, systems and applications to be outsourced, networks impacted, access methodologies, access protocols, application owners and system administrators be identified and reviewed for security vulnerabilities. It is preferable that these activities be completed during a feasibility phase. The vulnerability remediation strategy must be included in the contract business case, and the organization charged with vulnerability closure identified and initial timeframes specified. In addition, any systems containing highly sensitive customer data, company specific proprietary data, or special authentication requirements should be identified. An outsourcer organization must be responsible for collecting, and maintaining the aforementioned information. These resources will facilitate the development of a transition plan and risk mitigation strategies.

The majority of outsourcing agreements are terminated early. [10] A back out strategy must therefore be negotiated at contract inception. This includes the retrieval of any methods and procedures, documents, source and executable code, company proprietary security or development standards, code libraries and data stored off site. It is important to have processes set in place to block user IDs and privileges, and remove outsourcee access at network boundaries[11]. Another benefit accrued from the back out plan is that it can also be used as the template for the activities that will have to accompany the conclusion of the contract even were the arrangement to last to the end of its negotiated lifespan.

There are many methods to transfer information between companies. It is even more important to develop standards that will be used to exchange highly sensitive information. Transfer methods may include: fax, electronic mail, electronic file exchange, instant messenger, on-line meetings, and paper documentation. Any transfer method that may be used must have its rules for proper use (parameters) defined. For example, the outsourcer's internal Instant Messenger client might only be available for users who are connected to the outsourcer's network, but cannot be employed by users not directly connected to its network.[2] .[12] Encryption standards and practices must be identified, if applicable, and arrangements for key and certificate exchange and storage must be made. Encryption key lengths may be different due to regional variations in permitted key lengths worldwide. Alternatively, it is possible to transmit data securely over private channels or through the use of ssl connections where the certificates on only required on the receiving systems.

In order to save costs, the outsourcee may wish to subcontract some of the work. Language should exist in the contract that grants the outsourcer approval on all proposed companies and locations. No permission should be extended for subcontracting or off shoring without the express approval of the outsourcer Company. Such a policy may be necessary to protect a sensitive application or sensitive data contained within the application.

[2] Care must be made when permitting an Instant Messenger product because security safeguards are often bypassed

The following checklist identifies areas that should be reviewed prior to the finalization of an outsourcing and/or off-shoring agreement. This list is not meant to be exhaustive and other items may be needed according to the type of work performed:

- Ensure non-disclosure agreements are in place (individual and corporate). These agreements will also be required if any work is outsourced to another company. This includes companies performing long-term storage activities.
- Identify which company will supply the personnel supporting the contract. If the personnel will come from the outsourcer, how will they be transitioned over to the new company? An exit interview should be scheduled, and outsourcer proprietary information not necessary for the individual's new responsibilities must be collected, and unneeded system access removed.
- If the personnel whose work will be outsourced/off-shored are to be terminated, knowledge transfer sessions must be scheduled, and systems secured to prevent sabotage. This can include the removal of administrative authority, restriction of access into sensitive systems, reviews of audit logs and security software logs, and removal of login IDs from critical systems. If there is a significant concern about sabotage, then removal of access privileges may be warranted prior to the effective date of the contract.
- Identify where the new users will physically and logically perform their work. Identify access control methodologies for access into/out of the outsourcer's network.
    - If the users are working in outsourcer work areas, contractor type badges must be issued, and all employee badges collected. Identify acceptable access methodologies for outsourcee personnel to access the outsourcee corporate resources while on the outsourcer's corporate infrastructure. This access may include the use of VPNs (in single or split tunnel mode), private channels between the companies, outbound modem access or may not be permitted at all.
    - If the users will be working in outsourcee space, other questions for resolution include whether they will be using dedicated resources, housed on separate LANs, data stored on separate media and how will non-contract employees who visit the space be identified and escorted? It may be more difficult to validate work conditions if the work is performed out of the country.
- Define the topology of your network and sensitive LANs. Identify systems where non-company employees will need access. Establish listings of affected systems, system owners, administrators, and access protocols. Determine what external resources will be required to support the

contract. Establish guidelines for non-outsourcer computing equipment that may be connected to the outsourcer network.

- Agree upon security policies and best practices. Identify authorized individuals for policy interpretation and the submission of policy modification requests. Establish security policy training programs for affected personnel. Begin work to identify additional areas where security countermeasures will be needed because of the outsourcing and/or off-shoring effort. Ensure that the cost of implementing these countermeasures are incorporated into the business plan, and then tracked until they are implemented.
- Establish an issue resolution board with representatives from all affected companies. Best practices standards should be developed and distributed once resolutions have been issued.
- "National Security" issues may need to be addressed. This may have consequences in the areas of system access, employee background checking, and encryption of stored data. This will vary country by country and multiple policies may be required.
- Customer proprietary information must be defined and safeguards established. Develop training materials and roll out appropriate safeguards and standards to all affected personnel. Distribute contact information so users have a single point of contact for clarifications or interpretation of data.
- Agreements on data handling and data transfer requirements must be achieved. They should identify any portable electronic devices (e.g. personal digital assistants, remote e-mail retrieval devices, and mobile phone) that can be used, and safeguards that should be implemented to secure the devices.
- What electronic transfer of information including Instant Messenger, email, fax, or file transfer is permitted?
- Create Security Incident Response Teams and procedures for them to follow if the teams are not currently in place. Develop and rollout guidelines to all personnel outlining what incidents need to be reported, which Response Team should be notified, and within what timeframes must the notification be made. Develop hand offs between the Incident Response Team and local law enforcement personnel.
- Roles and Responsibilities of all personnel must be defined. The authentication and access control requirements should be identified based on the user's role, and into which systems he/she requires access. Identify what systems, applications, and permissions the users will be authorized to access.
- Establish guidelines for outsourcer to review system configuration, logs, security auditing software reports, and stored media. Points of contact must be identified from all impacted organizations.
- Identify processes for data to be transferred between the outsourcee and any company that it is subcontracting work. Define the documentation that must be kept and the interval over which the data should be retained.

Implementation Issues

The implementation phase of the contract will highlight any issues not identified during the feasibility (if performed) and contract negotiation phases. It is necessary to maintain a joint issue resolution team to identify and assign resources to work newly identified issues. The majority of issues fall into personnel, data handling, secure network access and network areas. In addition, software deployment and patch management practices will need to be instituted, regular review of audits (logs and results from audit software) must be completed, and a Centralized Incident Response Process implemented.

Personnel:

The outsourcer Company must retain some control over the personnel who are supporting its work. This can be accomplished by requiring background checks (to the extent permitted by law) of the contracted personnel[13]. Enhanced background checks may be required for those individuals who work on sensitive systems or special access (e.g., administrative rights). In addition, all personnel supporting the effort may be required to sign an individual non-disclosure contract, and participate in a review of the outsourcer security policies and practices. The policy review should occur at least every six months to ensure contracted employees are familiar with any policy changes. A formal application and access approval process should be established for new feature development and current application modification. A user termination process must be developed to ensure users are removed from systems and reminded of the non-disclosure agreement that is in place. The process should also insure that user login accounts are removed, and that any hardware is returned and is checked for viruses so it can be re-deployed.

If personnel are the shared between multiple supporting companies, data separation standards must be in place to prohibit the co-mingling of data. This may require the use of separate work stations/personal computers for each company supported. Dedicated resources and LANs may be required due to the sensitivity of the information and systems supported.

A determination must be made where the contracted employees will perform their work. If they are co-located at the outsourcer's location, they must receive security credentials to access the corporate infrastructure and buildings. In addition, methods for the contracted workers to access his/her home network must be defined. This could be made through the use of an outbound VPN, or connectivity over a private facility to the other company. It may be preferable to move these employees onto their own LAN so outsourcee company resources can be available locally.

Outsourcee employees who are housed at non-outsourcer locations must be provided access to those internal outsourcer systems, applications, and information storage areas required to perform his/her job. Physical access to outsourcer-related resources must be controlled and audited. This includes non-outsourcee personnel such as cleaning crews, telecom managers or hired security patrol personnel.

Data Handing:

The establishment of data handling procedures is critical, especially if data, software, or design specifications will be housed on non-outsourcer systems and desktops. Standards must be developed in the data exchange (electronic and paper), what data must be retained and for how long, on what media the data will reside, and when the data can be discarded through approved methods.

Information that is no longer required must be destroyed or returned according to the security standards established by the contract. Destroying may include shredding paper, degaussing floppies and tapes, or physically destroying the devices. An audit procedure must be followed to ensure that the information has been destroyed or returned. At the end of the contract, personal computers and servers may be re-imaged to ensure that all outsourcer proprietary information has been removed.

Electronic information between the companies should be sent via private channels (dedicated line or VPN), or encrypted with a key strength of at least 128 bits. The data encryption standards are country dependent, and it in some regions it may not be possible to use encryption[14].

In those cases where resources are shared between companies, system development must be performed to ensure that Company One's data can easily be segregated from Company Two's. Each company's information must be kept in such a manner that it can be easily separated, and held for long term storage on separate media. Additional development may be needed to restore archived information after technology or operating system upgrades.

Procedures must exist to protect information housed in PDAs, Blackberries, cell phones and other portable devices. Devices should be secured when not in use, security software installed and passwords enabled. If these devices are compromised, the Incident Response team must be notified.

Transfer of hard copies of documents must be sent using a service that permits in-transit and delivery auditing. Packages should not be delivered without a signature attesting that the information was received. Sensitive information should be sent in a double envelope, so that any tampering would be evident.

Due to time zone considerations, it is important to ensure that the recipient is available to collect the fax, or that the fax is sent to a secure location. Third party fax services that deliver the contents via email can also be considered, providing the company meets or exceeds the agreed upon security policies and practices.

Secure Access into the outsourcer's Network:

It is not always possible for the outsourcee employees to perform the work on the outsourcer's network, especially during off hours and emergency support situations. As a result, a secure remote access methodology must be implemented utilizing individual user authentication, audit capabilities and access control lists. The sessions must be logged and reviewed on a regular basis. This can be achieved using a firewall that supports strong or two factor authentication (such as CheckPoint[15]or Cyberguard[16]), a single tunnel VPN that supports strong, two factor or individual authentication (such as Nortel[17] or AT&T Global Network Services). Care must be made taken because malware may have been introduced into the outsourcer's enterprise by machines connecting through VPNs. Implementations have also been achieved using CITRIX servers instead of firewalls to lock down access with the use of Secure Computing Safeworld tokens[18] or Radius tokens[19]. This non-firewall solution may not provide sufficient auditing, or access control at the network boundary.

Outsourcee personnel visiting the outsourcer's location can introduce virus, worms and other malware to the outsourcer's network. Policies need to be established, communicated and implemented prior to permitting non-resident personnel access to the outsourcer's network. Additionally, it may be necessary to provide remote access back to the outsourcee's home network for time reporting, corporate methods and procedures and email. At a minimum, up to date virus detection software must be running on the personal computers, as well as restricted access precautions, prior to establishing any data connections.

Network:

The access required by the outsourcee to perform his/her tasks will have been defined during the feasibility and contract negotiation phases. A complete network diagram will be needed to define the agreed upon network boundaries, any specialized network segments, IP addresses of the application systems, key routers and systems such as the placement of name servers and Microsoft Windows domain controllers that will be part of the work effort. This information will be used to design firewall rules and other access control lists used to secure the outsourcee network and systems.

The safeguards necessary to protect the outsourcer's network will vary according the access needed by the outsourcee to perform the required tasks. Implementations to achieve the desired security protection may include network

segregation to restrict access to specific resources, creation of network segments where a higher level of access control is required, and use of DMZs for data transfer.

It is often convenient for users to post required information on shared drives. These are often deployed with little or no auditing capabilities or access control, thus permitting information to be viewed by anyone who has access to the network. Here, specific access control and audit mechanisms should be deployed.

A change in the corporate infrastructure may be required to also support domain and DNS services. A DNS proxy residing in a DMZ can permit the resolution of DNS, but prohibit the mining of the DNS. Additionally, specific policies concerning domain trusts must be established. The deployment of two-way trusts should be minimized, and other mechanisms should be implemented to protect domain resources, such as requiring users to authenticate to outsourcer's domain.

Life of the Contract Issues

Once all of the systems and personnel have been put into place, a change control process must be established to ensure that the system access, permissions granted, and network access remains current.

Personnel change control processes must include the capability to add, change or delete personnel assigned to the account. The process must continue to document system access and permissions granted, identify building(s) where the individual is granted access, and devices used by the individual to gain physical and network access. There must be a master database of record that defines the individual's role, function and system access.

Application IP addresses are often changed over the lifetime of the network. This information must be communicated to the access control management group to ensure the appropriate modifications at the network boundaries are made. Changes may include updates to router access control lists, firewall rules, VPN user groups, and changes to records supporting token or other access control devices. These changes must be logged and kept until after the termination of the contract.

Once new development has been completed, a formal change control and software development process must be followed. The change control requests must be maintained through contract termination. This software process should also include minimum standards for maintaining the old generics of code; regression, unit, system and user acceptance testing requirements; and documentation development, delivery of software, and a back out procedure in case the software does not function as defined. A Modification Request process must accept immediate change requests for security fixes.

Patches, especially security patches, must be tested to determine if the patch will harm the applications. A patch management task force should determine which patches need to be installed, what trusted site should be used to down load the patches, and what installation metrics should be in support of the outsourcing effort.

Security logs and audit software review must be reviewed at least monthly by the designated security and/or system administrative organization. Vulnerabilities must be identified, and plans must be developed and implemented to correct the problems, which appear. It should be noted, moreover, that centralized audit software could be installed to reduce the amount of manual labor required to complete the review.

An Incident Reporting Organization, designated under the centralized contract must be notified of all security incidents including virus outbreaks, unusual patterns in logged traffic, and suspected break-ins. The Incident Handing Organization, a specialized group within the Incident Response Team, meanwhile, will provide the interfaces between the outsourcer and the local authorities.

Disaster recovery and business continuity procedures must be documented and put into effect. Emergency system access procedures must be developed with logging and audit capabilities. These drills should be performed at least semi-annually.

Termination of Contract Issues

To smoothly terminate the relationship without causing harm to either security or business, an exit process must be documented and outsourcer personnel assigned to ensure that the processes are followed. An audit of all information and systems must be performed to ensure that all items have been returned or destroyed according to the contract. If the information was to have been destroyed, the records concerning its destruction must be provided. It is often preferable to employ a trusted third party to oversee and validate the destruction of information and media.

Outsourcer proprietary information that has been in the outsourcee (or long-term storage company hired by the outsourcee) must be returned or destroyed according to the terms specified in the contract. Contract language, it should be noted, must be explicit as to whether the proprietary information contained on backup tapes or other external media must also be included. It is important to follow the outsourcer's and local government policies and regulations to determine how long records must be kept. These rules may vary country by country.

The personnel who will be continuing to perform the current tasks must be identified and notified, and necessary information exchange completed. If personnel are returning to the outsourcer, a security policy refresher may be appropriate.

The removal of access into outsourcer applications, systems and network must be coordinated in such a way as to ensure business continuity. This includes the permissions granted at network boundaries (router, firewall, VPN rules, and access through authorized modems), superuser (root and admin) and user account removals, and the return of any physical access devices such as badges, swipe cards and tokens. It may be preferable to disable accounts until the completion of the termination process prior to the removal of accounts. This will ensure that critical information will not be deleted off the systems, and short-lived access can be granted in case of emergencies. These accounts can be granted with specific life spans and limited user rights. On-going outsourcee support should be negotiated, including service level agreements, duration of support, and system and network resources identified. The access methodology must be capable of being audited, as well as documented and tested. This may require the outsourcee be at the outsourcer's location because a secure remote access methodology is unavailable.

If appropriate, computing assets need to be transferred back to the outsourcer. Care must be used in removing any additional access that may have been provisioned, and the system must be inspected to ensure that it meets the outsourcer's current security standards for patches and virus control. If the hardware is not returned, the developed software should be staged on similar platforms to identify any issues, which may arise. All returned software, executables and other electronic information must be tested using the outsourcer's antivirus software prior to being re-deployed on its company's assets.

Activities required to terminate the contract must be performed in such a manner as to permit work to continue while re-establishing an outsourcer environment to perform the returned tasks. Care must be used when transferring personnel back from the outsourcee, returning hardware and software, and disconnecting access into the outsourcee enterprise.

Summary

In order to successfully execute an outsourcing and/or off-shoring contract, security safeguards, processes and policies must be agreed upon by all parties, and integrated into the negotiated contract. The contract and identified security policies will have to govern all activities that will be performed by all

parties, and, furthermore, a contract and policy modification process must accompany those policies. A steering committee must take responsibility for addressing items, and a point of contact established for dispute resolution and security interpretation.

The life of the contract phase is responsible for maintaining and/or improving the pre-contract level of security, and ensuring that information concerning access control, personnel, network architectures and data protection is kept current. There are often issues with this phase because adequate personnel are not assigned to complete the activities required.

The contract termination phase is responsible for restoring the systems, networks, data and personnel to their pre-contract states. This state may, of course, be reached prematurely if the contract is cancelled. As a result, a back-out and contract termination strategy must be established during the feasibility phase.

A successful outsourcing and/or off-shoring experience requires co-operation from all parties and agreements on the security policies and interpretations that will be used. In addition, planning must be done to ensure modifications and contract are completed in a timely manner, and additional funds are allocated to implement any changes to the enterprise necessary to achieve the desired level of security.

---

[1] Overby, Stephanie, "Staff Alert", **CIO Magazine,** May 1, 2003
URL: http://www.cio.com/archive/050103/staffing.html?printversion=yes
[2] Ambrosio, Johanna, " Experts Reveal the hidden costs of Outsourcing", April 23, 2003
URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci895398,00.html
[3] Gongloff, Mark. "U.S. Jobs Jumping Ship. Cheap Labor is not just for manufacturing any more – is your job heading overseas too?" May 6, 2003.
URL: http://money.cnn.com/2003/05/01/news/economy/jobless_offshore/
[4] Tham, Arthur," Security Web Digest: Outsourcing A Risk? US Networks Safer than Before, Sabotage to Combat Piracy…" May 2, 2003
URL: http://security.ziffdavis.com/print_article/0,4281,a=41324,00.asp
[5] Hoffman, Thomas and Thibodeau, Patrick, "There's more to consider than cheap labor" April 28, 2003
URL:
http://www.computerworld.com/managementtopics/management/outsourcing/story/0,10801,80662,00.html
[6] Hurley, Edward, "It makes sense to outsource IDS, experts say", **SearchSecurity,** Nov 12, 2002
URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci862918,00.html
[7] Hurley, Edward, "The Pros and Cons of Outsourcing antivirus protection", **SearchSecurity** November 26, 2003
URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci866024,00.html
[8] Christie, Linda, "Outsourcing with a new twist", **SearchSecurity,** July 11, 2003
URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci754618,00.html
[9] **e-Zest Solution Pvt, Ltd**
URL: http://www.e-zest.net/Outsourcing_central/outsourcing_issues.html
[10] Rosa, Jerry, "Happily Ever After" **eWeek Magazine,** August 20, 2001
URL: http://www.eweek.com/article2/0,3959,103866,00.asp

[11] "Breaking Up Is Hard to Do", **CIO Magazine**, March 2003
URL: http://www.cio.com/archive/030103/outsourcing_break.html
[12] Hurley, Edward, "IM putting enterprises at risk to viruses, attack" SearchSecurity**,** May 7, 2003
URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci822034,00.html
[13]Kendell, Sandy, "Employee Screening: How Little is Enough?"
URL: http://www.csoonline.com/talkback/050503.html, May 5, 2003
[14] Lieb, Jeremy, "The Regulation of Data Encryption Technologies: *Butting Heads...and Missing Completely"*
URL: http://www.commerce.net/research/reports/1997/97_18_n.html
[15] **CheckPoint**
URL: http://www.checkpoint.com/press/1997/newlevel0902.html
[16] **Cyberguard**
URL: http://www.cyberguard.com/pdf/cyberguard_datasheet_family.pdf
[17] **NORTEL**
URL: http://www.nortelnetworks.com/products/01/contivity/index.html
[18] **Secure Computing**
URL: http://www.securecomputing.com/index.cfm?sKey=1158
[19] **CITRIX**
URL: http://knowledgebase.citrix.com/kb/entry.jspa?entryID=2362&categoryID=135

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event