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.

Vendors and External Outsource Providers How Safe is Your Companys Confidential Data

Let us assume your business is fairly accomplished in the Risk Assessment evolutionary ladder. Perhaps your company already assesses its network configurations regularly, all the applications in use have been reviewed for stringent security guidelines, maybe the IT team has even classified all your corporate information assets, and the vulnerability assessments are complete. Does this mean the CIO can relax? Is the business safe? Is your network or information accessed by a third party vendor? Where is your information...

Copyright SANS Institute
Author Retains Full Rights

AD

Security Assessments at

Vendors and External Outsource Providers -

How Safe is Your Company's Confidential Data?

© SANS Institute 2004, Author retains full rights.

Written by Stan Gucwa
GSEC Practical Version: 1.4b (Option 1)
30 November 2003

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

Abstract

Let us assume your business is fairly accomplished in the Risk Assessment evolutionary ladder. Perhaps your company already assesses its network configurations regularly, all the applications in use have been reviewed for stringent security guidelines, maybe the IT team has even classified all your corporate information assets, and the vulnerability assessments are complete. Does this mean the CIO can relax? Is the business safe? Is your network or information accessed by a third party vendor? Where is your information being managed, stored or processed? Is it always on your network? Is it always within the walls of your company? Do you outsource any business functions? Is any of your client's personal information shared with a third party? Do you have any business-to-business connections?

If the answer to any of these questions is "yes", then you have to realize that your information may only be as secure as your vendors or business partners protect it. What do you do to assess them? Are you authorized to assess them? This paper will cover some of the important considerations that should be made to keep your corporate assets, intellectual property and most of all, your customer's personal information secure.

Introduction

The complexity and implications of a solid security posture become very important quickly when you assess the true location of the information your company is obligated to protect. The threat of identity fraud is a growing concern. As reported in a recent article from SearchSecurity.com; "A recent Federal Trade Commission report said that 27.3 million Americans were victims of identity theft during the last five years (including 9.9 million last year alone). Such activity cost businesses almost $48 billion last year." [7] The amount of disgruntled employees due to cutbacks and potential job loss is on the rise as a serious threat. The rising cost of technology and business' desire to improve the bottom line is fostering the business decision to outsource more and more business functions. That decision gives more and more individuals access to the company's confidential information. The locations of these vendors or external outsource providers could be down the street, in the next state, across the country or offshore on foreign soil. How does one provide some assurance that these vendors or outsource providers have properly screened their employees that are accessing your confidential information? In order to protect themselves, corporations are starting to perform due diligence assessments on their technology vendors and external outsource providers.

Your company may have a respectable security budget and work diligently to safeguard company proprietary information and the personal information of your customers, but what has it done to assure the information is secure outside the

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

four walls of your company. The scope may be more manageable if you are operating a small business with a few vendors. However, the task for assessing the situation grows quickly if you have a larger corporation with hundreds of vendors and external outsourcing providers. Proper measures must be taken to assess the risk of sharing your confidential information with others. Otherwise, the consequences and potential loss to the business due to a security breach or unauthorized disclosure of information at a vendor site could lead to litigation relating to breach of contract, disruption of customer service, loss of customer accounts, loss of income, loss of reputation or market share or negative publicity, prosecution, fines, or other actions that restrict ability to conduct business, etc. The list gets longer and longer as more systems in various sectors of business continue to automate business processes and provide more and more external parties, which could be customers, vendors or business partners with access to their information.

Requirements

The path to success begins with documenting the high-level process. Draft an oversight program to monitor and perform assessments on vendors and external outsource providers that manage, process or store your confidential information. The process will have to integrate with your legal department so that the correct contractual requirements are defined with your vendors and external providers at the start of the business relationship. Many times the corporation will be playing "catch-up" because a contractual relationship already exists and makes no reference to security requirements or the possibility of annual onsite assessments. In this case, the additional required terms may have to be addressed between the parties involved and added to the contract at the time of renewal. If you have a sizeable company, the supply management team or purchasing department may end up being the link to proper management of your external business relationships since they may maintain the schedule for financial assessments and contractual maintenance.

It would be prudent for the supply management team to be performing financial assessments on all the vendors and external outsource providers that access, manage or store your confidential data. If any one of them is providing all or part of a critical business process and they are not financially sound, then several questions would arise. If they go out of business do you have an alternative source? Can the function be performed internally if required due to emergency? If the vendor is involved with a critical process, has an exit strategy been documented to protect the business? And in the context of this paper, if they are in financial trouble, what is the ramification to the security budget and security posture of their company?

Depending on the size of the company this assessment process may be shared across corporation and its final departmental place of rest with regards to

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

responsibility may vary from company to company. The one common thread will be the requirement to integrate an Information Security Officer, CISSP, GSEC certified or equivalent person into the process to assist in the assessment of the vendors and external service providers to assure their security practices are at a level competent enough for the level of classification of data they are protecting.

Key Points of the Process

The business needs to maintain a documented inventory of all vendors and external outsource providers that could possibly have contact or access to the company's confidential information. This inventory must be kept current with contact names and numbers. This is an operational portion of the process that is ongoing and must be maintained as new vendors are added, deleted or have changes in the scope of services that they provide to your organization.

The next step would be to contact the company and find the appropriate person or personnel to meet with in order to evaluate their security posture. This could be one individual for a small company and could lead to a rather lengthy list in a large corporation (ie. information security officer, physical security manager, facilities manager, CIO, CEO, data network manager, etc.). During your initial discussion with the business contact of the targeted company to be assessed you would want to explain your concerns for safeguarding your company's confidential information and discuss your new corporate policy to execute security assessments on all of your external supply base that manages, stores or processes your confidential information.

This would be an appropriate time to check with your internal staff to see if a properly executed Non-Disclosure Agreement (NDA) has been executed with the specific company. A Non-Disclosure Agreement should be collected and retained on file for your entire external supply base that manages, stores or processes your confidential information. The Non-Disclosure Agreement is a contract whereby both parties sign the document to agree that they will not disclose certain information, under the terms of their business agreement, to any other external parties. The Non-Disclosure Agreement has been working well in the United States and are quite common between companies that share or disclose proprietary information amongst one another. There are laws in place like the Industrial Espionage Act of 1996, which would make non-authorized disclosure of proprietary information a criminal offense. However, most of our laws in the United States would not apply to non-U.S. citizens that may reside or be acting on foreign soil. Therefore, the sending of confidential information to offshore locations adds another layer of complexity to the assessment process and the precautions that must be considered prior to letting proprietary information leave your company's premises.

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

The diverse breadth and scope of company policies, standards and procedures that may be covered and shared between parties during a security assessment will definitely require a Non-Disclosure Agreement. The information collected during the assessment itself should be classified as confidential within your company and only be shared with security and business staff that have a "need-to-know" for the information. After all you are basically assessing a company with the goal of determining where their shortcomings are within their physical and logical security parameters. Allowing that information to get into the wrong hands is a security risk in itself, so please take appropriate measures to safeguard your vendor's shared information after they were willing to let you in their circle of confidence to understand their security practices.

The growing concern and requirements placed on businesses today by new legislation such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act of 1999, or Sarbanes-Oxley Act of 2002 may have some of your vendors and external providers improving their security posture before you placed your first call to them. They may have a number of their customers inquiring about their security posture and use of internal controls to safeguard confidential data to the point where they hired an external auditor to perform as SAS70 audit.

For those not familiar with this audit, SAS 70 is the abbreviation for "Statement on Auditing Standards (SAS) No. 70." The following excerpt is taken directly from the SAS70 website www.sas70.com[9]:

> <u>SAS 70 Overview</u>
> Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS 70 audit or examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. [9]
>
> SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.[9]

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

If the vendor or external outsource provider does have a SAS70 performed on the location that performs a service to your company make a formal request for a copy of the SAS70 Report. Upon receipt, review the document carefully and determine if any significant findings were reported. If no significant findings were documented, this expensive external audit may give you some assurance that your data is being treated with adequate controls and that reasonable security measures are in place to protect your data. If any minor findings were present, make a note in the company's file you are keeping such that if an onsite assessment is performed at a later date you can validate that the finding was corrected adequately while you are onsite. In any case, depending on the corporate budget and resources available there is no replacement for performing an onsite assessment and seeing the process in place firsthand.

The Assessment

The onsite assessment process, security audit, security posture evaluation or whatever politically correct and contractual obligated term you would like to you use to refer to it, should be a documented standardized process. So, if your company is at a level where it is required to be audited by external parties the process will meet their criteria for being a mature formalized evaluation. This is usually in the form of a vendor assessment checklist that covers the basic security topics. There is some controversy regarding the approach to use in these assessments with regard to sending the checklist of questions to the company ahead of time, my belief is that you should not share your list of actual questions or points of assessment until you are onsite. The reason for this is that the company may have a fire drill to prepare for the assessment and try to create policy, practices and perform quick fixes to cover your topics prior to your arrival. While the increased interest to satisfy you as a customer may at first seem commendable, security is not something that is solved overnight or in a week to prepare for an assessment. I prefer to leave the company with a basic overview of areas of interest and get a true understanding of their security awareness or a "snap shot of business as usual" [4] from the visit.

When planning the date for your onsite visit, you should make a formal request for the required personnel you will need to acquire the information needed to ascertain the maturity of the vendor's security policy and procedures. The typical key members of the vendor's staff you will most likely require are the Facilities Manager, Data Center Manager, Network and Systems Managers, Security Manager, COB Coordinator, CIO and Business Relationship Manager.

During the assessment, you would want to physically review the vendor's Security Policy or Standards, Change Management Procedure and their Continuity of Business Plan. Verifying that the company does indeed have these three key documents in written form with current revision dates would provide a large insight into the level setting process for the rest of the assessment.

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

The following outline is a generic outline of the typical topics reviewed and assessed during an onsite visit, the list may be adjusted based on the sector of business you are assessing, criticality of the business function that the company provides and degree of information content that is shared with the vendor or outsource service provider:

Facility and Physical Building Access & Security

- Access points to the building and restricted areas
- Video camera placements, monitoring and handling procedures
- Physical access by employees and non-employees to both building and restricted areas
- Power backup capabilities
- Disaster prevention and recovery both physical and electronic
- Process and procedures for electronic and physical access
- ID authentication, monitoring, maintenance and auditing of both physical and electronic access

Infrastructure, Systems & Technology

- Anti-virus, firewalls, intrusion detection systems and operating systems
- Information classification, authorization, monitoring and auditing
- Upgrades, hotfixes and patch management
- Entitlement reviews
- Data transfer and encryption
- Information security incident detection and handling
- Change control management, monitoring and auditing

People, Policy, Procedures, Compliance & Audit

- Duties and responsibilities of key personnel, such as administrators, Information Security Officers, Security Officers, persons with access to key systems or data
- Audit information such as frequency, findings, corrective actions or plans, risk acceptances, etc.
- Duties and responsibilities of employees and non-employees (ie. consultants)
- Use of background checks for individuals with access to classified information
- Any documented procedures, policies, or practices related to any of the topics above

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

Internet (if providing web hosting or web application services)

- Assessment of the data available via the web servers
- Application architecture
- Method of authentication (active directory, LDAP, etc.)
- Intrusion detection systems
- Annual vulnerability assessment (ethical hack, appscan, etc.)

When conducting an onsite review, it is usually best to start with a meeting to cover basic introductions and review the topics that are desired to be assessed during the visit. The next step would be to do a physical tour of the entire facility, especially the data center. During the physical tour special areas of interest should be; all external doors used by employees, telecom closets, access control and location of all LAN switches and intermediate data frame racks (key infrastructure points), where power and network lines enter the facility, and depending on the facility even inquire how access to the roof is monitored and controlled. In every regard you must have a determined agenda based on the company, business function that they provide, and availability of the personnel you need to interview to obtain the information you are seeking; yet still be willing to be flexible and compromise your time to be as efficient as possible to achieve the goals of the assessment.

Any issues arising from the review should be shared with the vendor or external outsource provider both verbally at the time of the visit and in a subsequent summary report. In order to maintain a good business relationship with the vendor, you need to be as upfront as possible with any weaknesses you may uncover. The summary report should be drafted in a form that will illustrate the relevance of the assessment. Therefore, it should include any potential findings, the risk associated with that finding and possibly a recommendation or best practice to correct the finding. Once a final summary report has been issued, the vendor should be asked to respond to any issues that have been identified within a two to three week period. When the responses are received they should be reviewed via a conference call with all parties involved to assure the response is complete and the timeline to closure is reasonable. Make sure someone in your company is assigned the responsibility to be the liaison with the vendor to assure any concerns are tracked to closure within a reasonable timeframe.

Lessons Learned

The vulnerabilities that may be uncovered at some of your vendors during your initial assessments may be quite alarming. This should be expected in the beginning of such a program. Many companies still have low hanging fruit that needs to be cleaned up. This should be viewed as a cleansing process in relation to the benefit everyone will receive in terms of improved security. Be leery of the companies with less of a security posture that may tend to view the assessment as more of an intrusion. The hard fact is they don't appreciate

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

having an outsider tell them about their vulnerabilities, but without your intervention they are likely to do nothing. You are doing them and their customers a great justice. Other companies that already have a heightened security awareness will view the assessment as a positive that they are receiving a security assessment for gratis. The fact that your company initiates such a process will immediately raise the bar of what is expected from companies that desire your business. This will assist to elevate the overall awareness in the industry itself of what should be expected to protect confidentiality, integrity and availability of your company's confidential information.

The type of response you receive to your summary reports will give an indication of which vendors are interested in being a "going-forward" vendor in your business versus those that just don't see the importance and are waiting for an incident to occur to help them find a reason to be more secure or go out of business.

Summary

The implementation and execution of a documented security assessment process will provide an excellent return in the risk management process to minimize the chances of a breach in the confidentiality, integrity or availability of the information your company is obligated to protect. Extending the obligation to your vendors or external outsource providers has inherent risk, but a properly executed annual security assessment at their physical site will work to minimize that risk. The implementation of such a business practice will work to heighten the security awareness of the companies involved. As more of corporate America comes to understand the importance of keeping critical information secure, and now guided with the assistance of recent legislation (ie. Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act of 1999, and Sarbanes-Oxley Act of 2002) the momentum of growing security awareness is gaining speed.

The initial onsite assessment may be viewed as a kind gesture in order to maintain business relationships, possibly as a valuable security evaluation that is free compared to what the cost could be if they contracted a consulting company to provide the same service or an opportunity to spread the concept of defense-in-depth. In any scenario, the outcome should be a shared awareness of the possible vulnerabilities to each company and the information that has significant value to both parties involved. The process of finding gaps and evaluating the best corrective action to remediate the gaps is a learning experience that makes both companies more secure and provides both with a better understanding of the intricacies of their business processes going forward. This is definitely a worthwhile endeavor for the businesses involved and for the battle of keeping customer information secure.

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

References

1. Campbell, Phillip L., "Survivability via Control Objectives". Position Paper for 3rd IEEE Information Survivability Workshop.
   URL: www.cert.org/research/isw/isw2000/papers/24.pdf

2. LanWrights, Inc. "Security audit action list for CIOs". TechRepublic. 16 July 2003.
   URL: http://techrepublic.com.com/5102-6296-5054775.html

3. Bruck, Michael. "Why You Need an External Security Audit." 17 March 2003.
   URL: http://www.entrepreneur.com/article/0,4621,307326,00.html

4. Shore, Joel. "Inside a security audit". 22 October 2003.
   URL: http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,86354,00.html?f=x583

5. Unknown. "Network Security Myths."
   URL: http://www.apnafuture.com/IT%20Information/Articles/Network%20Security%20Myths/Network%20Security%20Myths.html

6. Pearce, James. "ID theft battle threatens Aust privacy: Experts." 11 July 2003.
   URL: http://www.zdnet.com.au/printfriendly?AT=2000048600-20276155

7. Hurley, Edward. "Coalition to help enterprises manage identities against theft." 25 September 2003.
   URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929447,00.html

8. CSO Magazine. November 2003. "Big Savings, Big Risk." Fitzgerald, Michael.
   URL: www.csoonline.com

9. "About SAS 70." Site last updated, 20 September 2003.
   URL: http://www.sas70.com/index2.htm

10. Harris, Shon. "CISSP Certifcation." McGraw Hill, 2002. ISBN 0-07-219353-0.

11. Crume, Jeff. "Inside Internet Security." Addison-Wesley, 2000.

© SANS Institute 2004, 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**