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.

Addressing and Implementing Computer Security for a Small Branch Office

In today's global environment, it is not unusual for large companies to establish a presence in locations throughout the country or the world. This presence may be a single individual or a small team working at a remote location. This paper will address the security issues faced by a small office accommodating staff reporting to the main location and visitors requiring "computer access".

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

Addressing and Implementing Computer Security for a Small Branch Office
Patria Leath
October 10, 2001
GIAC Level One Security Essentials GSEC Practical Assignment Version 1.2f

Implementing security measures and security awareness for a small branch office raises a different set of questions and provide some unique challenges than when one is implementing security for central or main location. Who determines the security policy? How is the policy enforced? Who implements the security? Local staff? Staff from the main site? Is it outsourced? In a location with different organizational units represented, who determines the cost of not providing security? There is no "one size fits all" solution. It is important to understand the issues and work within the organizational structure to develop awareness and policies that will comply with the global requirements of the organization while permitting the remotely located staff to work efficiently and effectively.

In today's global environment, it is not unusual for large companies to establish a presence in locations throughout the country or the world. This presence may be a single individual working at a remote location on a specific task or a small office. The case of an individual working in a remote location has its own issues. This paper will address the security issues faced by a small office accommodating staff reporting to the main location and visitors requiring "computer access".

Basic to this entire discussion is the background of the individual responsible for the day to day operations of the branch office. Frequently an office such as this may be staffed with individuals that are at this location for the convenience of the customer, the organization or themselves. They have their own work to complete and require varying levels of administrative and technical support. Generally, the organization's primary concern is a point person for "administrative" issues. Little thought may have been given to the computer and security infrastructure until something goes wrong. Then, the end user or an administrative assistant may contact a help desk or someone in their work group at the main location and attempts made to correct the situation. In some cases this may be a satisfactory solution, but does it represent the best use of resources? Has the "fix" compromised the enterprise security?

The goal of any security scheme is to find the balance between convenience and security, protecting the assets of the organization while not inhibiting the business processes. There must be acknowledgment at the organization's management level that this remote location requires time, attention and resources in order to prevent a breach in the security of the entire enterprise. That infamous "someone" must appreciate the importance of compliance with organizational security policies and develop security policies specific to the branch office. This could be a hard sell, since security is working well when nothing is happening, i.e. no virus attacks, intruders or compromised assets. Local security policies should be derived from the organizational policies but modified to address the unique situation of the branch office as well as the requirements of the various divisions or organizational units that have staff located at or utilizing the office. It is necessary for

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

this “someone” to have managerial oversight and responsibility for this office. They do not necessarily need to be located on site, but they do have to have responsibility, accountability and the authority to implement security measures.

This individual must then take steps to avoid the seven top management errors that lead to computer security vulnerabilities that are outlined on the SANS web site. These errors were identified by computer security experts and managers at a SANS conference in 1999 and hold true today. In reverse order they are:

Number Seven:	Pretend the problem will go away if ignored
Number Six:	Authorize reactive, short-term fixes so problems reemerge rapidly
Number Five:	Fail to realize how much money their information and organizational reputations are worth.
Number Four:	Rely primarily on a firewall
Number Three:	Fail to deal with the operational aspects of security; make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed.
Number Two:	Fail to understand the relationship of information security to the business problem—they understand physical security but do not see the consequences of poor information security.
Number One:	Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.

While all of these are important, addressing numbers one through three would go a long way to ensuring a secure computing environment. Assigning untrained staff to maintain security may be worse than having no security at all. They will have no credibility or authority and could actually introduce compromises to the system if not properly supervised by trained personnel. Investing in trained personnel, whether you train your own, hire your own, or contract with a managed service provider (MSP) is key to implementing a good security plan. The decision of whether to hire, train or outsource requires a lot of thought and tradeoffs. Is there someone currently on staff with the interest and aptitude for computer security issues? Would this individual be effective in the position with the appropriate training? How much training will be required to get this individual up to speed? What will it take to keep them current? Is there enough work and available funding to hire a new position? What are the pros and cons of outsourcing? How do you feel about giving a stranger the “keys to the kingdom”.

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

There is no easy answer, and one solution will not fit all situations. Perhaps a blended solution is the best. Under some circumstances, outsourcing may offer the best solution. By providing a detailed description of the company's requirements and defining performance standards, one should be able to find a company that will provide access to a team of specialists with current technical knowledge and abilities. Ideally, the customer will have access to a team of talented individuals and not be dependent on a single individual. Price will determine the level of monitoring and the response time provided by the MSP. The customer may be able to specify specific individuals that will provide service and will not have to deal with staff turn over or training. This should make routine monitoring and support as well as deploying new technologies easier. Key to this solution is finding a MSP that understands your business process and requirements, has a good understanding of the different available technologies, can communicate well with the lay person and, perhaps most importantly, demonstrates that they are trustworthy. Benefits to a MSP include the fact that Information Security should be their core business. This should enable them to be proactive rather than reactive. They will have a number or clients and therefore should have a more global perspective on Information Security. Negative factors to considering this solution may be the staff turnover at the MSP, the cost of the service, and the fact that a remote user in connected to the site, generally via the internet. In house staff will still be required to oversee the activities of a managed service provider and to ensure that security requirements are being met.

Hiring an individual to provide computer and security support may provide the greatest challenge. Finding an individual with the required expertise and keeping them interested and motivated can be a tough assignment. The ideal individual is aware of and trained in current technologies, understands the business and security requirements, communicates well with end users, and is not so focused on "bleeding edge" technology that s/he fails to properly accomplish the routine tasks at hand. However, they are looking for ways to improve the business process. The management challenge in this situation is encourage this individual to keep current in the field, ensuring that there is the correct balance of routine and interesting work, and that the pay is comparable to the current market. There is nothing as discouraging as running a shop with a revolving door with the "hire, train, leave" cycle. On the other hand, assigning the computer security tasks to untrained staff because they are "good with computers" can be equally disastrous. The majority of security breaches come from within the firewall. While some of the incidents may be due to disgruntled employees, others are due to improperly installed and configured software or patches that are not current. If the decision is to "grow your own", it is key to identify individuals with interest and aptitude, provide them with appropriate training and mentoring, and ensure that their activities are appropriately supervised.

Depending on the size and complexity of the requirements, a blended approach might offer the best solution. If the routine requirements are not sufficient to keep one individual fully engaged, the preferred solution may be training in house staff to perform the routine tasks such as monitoring the servers and managing the backups and providing end user support and calling in the professionals if something is amiss. Contracting with a MSP to address the more complex issues and implementations. The MSP could be

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

available on an emergency response basis as well as on a weekly or monthly basis to monitor the system. And, have the entire operation monitored by professional computer staff at the organizations main location. This would avoid the potential problems created by having a single individual responsible for the entire operation, provide for local attention to end users and routine tasks, have expertise available when required, and have oversight to ensure compliance with enterprise policies and requirements. A critical component to this scheme would be regular periodic audits by an independent agent to evaluate the overall security of the network, focusing on firewalls, servers, workstations and policies and procedures.

Implementing a solution similar to this would go a long way in addressing errors one through three as outlined above. However, a facet that has yet to be addressed is the end user. The end user is key to the successful implementation of any security plan. The overarching security policy will necessarily come from the corporate or main location. However, it is highly unlikely that the corporate policy would be effective at a branch office without some modification or adjustment. Key to a successful security program is end user compliance. Key to end user compliance is security awareness and education, coupled with a policy that demonstrates an understanding of the business process and the tasks that must be accomplished. A security policy that encompasses "best practices" while keeping the business objective in sight will meet with the most success.

This local security policy and operating procedures, along with network and hardware specifications should be documented and kept current. System documentation and logs are an essential tool, especially for the MSP or in the case support is required from the main office. Topics covered in this document should include the password procedures, virus update procedures, requirements for user accounts, requirements for guest accounts, resources available to visitors to the office. Operating procedures should also include a response plan to different events such as a virus attack, denial of service attack, or environmental incidents such as flood or fire. Outline the process followed when an individual leaves the organization. How long is the account kept? Another component should be a change log, documenting any changes or upgrades to the systems. A checklist of daily, weekly and monthly tasks demonstrates thorough work habits and are especially helpful if different individuals would be monitoring the network at different times. This would ease the sharing of information and let the someone know if an occurrence was typical, recurring with a certain frequency or under certain circumstances, or a sudden and unusual phenomena. The adage to "know thy system" is important, and slightly more difficult when responsibility is shared among different individuals.

Another aspect of a branch office is "the visitor" and remote user. The visitor may be a corporate visitor from another office or an individual with whom the organization has a business relationship. This visitor may show up with a laptop and just request to "plug in" to the network, or s/he may request access through local workstations. What resources of the branch office will be made available to these individuals? This should be addressed by the security policies and procedures. Visitors should be required to abide by local security policies, and this will be much easier to enforce with endorsement

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

by management. Configuration of a network segment to permit visitors access via a VLAN to the corporate office may be one solution. Local workstations with internet access without access to local networks may be another. Sharing passwords is not. The remote user that needs to access system resources from offsite is another potential security breach. Step must be taken to ensure that this user does not compromise information security by introducing a virus, letting in a hacker or permitting unauthorized access to company information. A solution to these challenges may be best met by a discussion with local office management, the organization's computer security team and the MSP to develop a solution that can be implemented securely and monitored for vulnerabilities.

Once a policy is in place, security awareness training for staff should be developed. Management support at this point is key to its success, especially if the office houses individuals with different reporting hierarchies. Each individual must hear from his or her manager that this is an important issue requiring his or her attention and cooperation. Additionally, the branch office must be aware of the security requirements of each organizational unit and, depending on the capabilities of the network, implement the most stringent. Successful training will require an understanding of individual work processes. Some of the processes will be common to all users, others will be unique. Appreciating and understanding individual requirements will aid in user compliance.

Security awareness training should cover procedures for passwords, response to viruses, physical security and an awareness of social engineering techniques. An effective password policy should meet certain complexity requirements. Most users would appreciate an explanation of why a password should be at least eight characters long and contain characters, numbers and uppercase letters. Explain why and how often they will be required to change the password. Share information on "acceptable use" and outline the consequences of "unacceptable use". Discuss computer viruses, the proper response and outline the office's virus protection plan. If users are required to update their own virus definitions, make sure that they understand the procedure and follow up periodically to ensure compliance. If the virus definition updates are pushed out to individual workstations and scans are automatic, let them know what they might expect. Let them know what may happen if they disable auto protect. Outline the back up procedures and advise them of the policy for backing up individual workstations. Make certain the individual user knows where s/he saves his or her files and how often they are backed up and how to request a special back up if desired. Inform users of times that they might be denied access to the network if the security procedures force users off the network at certain times (all you need is someone pulling an "all nighter" to meet a deadline for a deliverable and have them unexpectedly logged off the network. Talk about disgruntled). Educate users to social engineering techniques. Encourage them to report any suspicious or unusual activity or personnel. Present awareness training on a frequent basis, share current issues, and keep it concise. Communication on an ongoing basis should help to keep awareness high without crying "wolf". Explaining the importance of the security measures should aid compliance, especially if the explanation is designed to be "up close and personal".

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

Information security is not a static process but requires continual surveillance, auditing, patching and training. Default configurations and passwords should be avoided. Default path names and installation of sample code provide vulnerabilities. Patches and updates must be tracked and applied in a timely manner. Systems must be monitored for any unusual activity. There should be regular backups. Contingency plans should be developed and tested for feasibility.

There are many challenges facing organizations today. Computer security in branch offices is just one of them. There is no "one size fits all" solution. Any successful solution will require the identification of the "Responsible Person" and development of security policies and procedures that meet organizational requirements while keeping the business objective in site. There should be an acknowledgement that these policies are not static. They should be frequently reviewed and modified as needed to reflect the current business objectives, economic climate, corporate culture and operating environment. To be effective, these policies should "make sense", be communicated to all users and should be enforced through out the organization. There is also the challenge of finding the right kind of support solution. It is easy to make the mistake of assigning this "admin task" to an untrained individual without providing appropriate training and support. It would only be a matter of time before this would prove to be a fatal error. It is much better to be proactive and evaluate the alternatives of training current staff, hiring staff, and outsourcing. Steps should be taken to avoid the other common management errors of failing to understand the relationship of information security to the business process and failing to address the operational aspects of security. Find a solution that makes sense, and make network security everyone's responsibility.

Sources:

Control Data Systems, Inc. White Paper "Why Security Policies Fail". 1999. URL: http://www.securityfocus.com/data/library/Why_Security_Policies_Fail.pdf (October 2001)

Chetty, Synthil. "Outsourcing Security Management". April 10, 2001. URL: http://www.sans.org/infosecFAQ/policy/outsourcing.htm (September 2001)

Donston, Debra. "A Healthy Security Attitude". eWeek. June 10, 2001. URL: http://www.zdnet.com/enterprise/stories/main/0,10228.277133.00.html (October 2001)

Herring, Jim. "Network Security on a Shoestring". December 15, 2000. URL: http://www.sans.org/infosecFAQ/securitybasics/shoestring.htm. . (September 2001).

InfoWorld. InfoWorld Test Center Research Report, "IT Security". November 19, 2001. Pp. 47 – 57.

Lindner, Craig E. "Information Security Primer". August 18, 2001. URL: http://www.sans.org/infosecFAQ/securitybasics/infosec_primer.htm. (September 2001)

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

Lundquist, Eric: "Security: That Most Thankless Task" .eWeek. June 10, 2001. URL: http://www.zdnet.com/enterprise/stories/main/0,10228.2771376.00.html (October 2001)

Thompson, David. "The Social Engineering of Security". eWeek. June 10, 2001. URL: http://www.zdnet.com/enterprise/stories/main/0,10228.277132.00.html (October 2001)

Sans.org . "The Top Management Errors the Lead to Computer Security Vulnerabilities".http://www.sans.org/newlook/resources/errors.htm. (October 2001)

© SANS Institute 2001, Author retains full rights

Last Updated: September 3rd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced