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.

Security Considerations in the Merger/Acquisition Process

Those who work for a firm that acquires other companies or have undergone a merger understand there are a multitude of issues to cover before the deal is done. However, once the deal has been closed, the push to get both businesses connected and integrated can be tremendous. This document will focus on the high-level security issues that if included in the due diligence process, can help facilitate integration of the companies involved.

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Security Considerations in the Merger/Acquisition Process

By Anita Hartman

SANS Security Essentials GSEC Practical Assignment – Ver 1.2e

Those who work for a firm that acquires other companies or have undergone a merger understand there are a multitude of issues to cover before the deal is done. However, once the deal has been closed, the push to get both businesses connected and integrated can be tremendous. This document will focus on the high-level security issues that if included in the due diligence process, can help facilitate integration of the companies involved.

First Get the Background

Before determining where security gaps are between the companies involved, an understanding of what the organization being acquired looks like is key, as well as knowing the basic strategy behind the purchase. Once the background and strategy is understood, the types of security concerns will be more easily determined and plans for addressing any gaps can be documented. Included within this background information should be the following:

- Type of business
- Physical locations
- Organization charts
- Number of employees
- Computing environment
- Relationship moving forward

Type of business – Is the acquisition a diversification from the existing business the parent company is involved in? Will policies, standards or procedures need to be modified to ensure there is no negative impact on pulling the new business under the parent structure? For example, in the case of a financial services company, you will want to review privacy statements to determine promises made to Web site customers and users. The privacy statement will indicate the restrictions that will apply to the transfer of any personally identifiable information. Each industry has it's own set of rules, legislation, etc. that must be complied with – if diversifying into a new industry, security policies/standards may be impacted.

Physical locations – A couple of issues can arise over physical location.

- Does the acquisition reside in the same country as the parent company? If not, there are most likely laws specific to that country that will impact the parent company that need to be taken into consideration from a policy viewpoint, flow and exchange of information, etc. Cultural issues will also need to be taken into consideration as policies; standards and practices are revised for a consistent fit within the larger organization. Translating policy or

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

awareness materials into another language can be time consuming and expensive and may not be appropriate.

- If the acquisition is in another country, are there subsidiaries residing in other countries that will need to be addressed? The same issues from above will need to be addressed for each country the company does business in.
- If the acquisition is strictly a domestic one, is it in the same city/state or another location? If a different geographic location is involved are there state regulatory issues that need to be considered?

Organizational charts and number of employees – It helps to understand the structure of the acquired company. In particular you'll be interested in knowing if there is an Information Security officer or department and if so what the reporting relationship is to senior management. Reviewing the organization chart should allow you to identify key people that you may need to be working with. A red flag for a large organization would be if there is no mention of security under the CIO, IT or Audit areas. No matter what the size of the company, security can be a sensitive topic and you will want to carefully consider how to approach management on issues. Another item to think about is whether there is potential for attacks from within. After the acquisition is announced some employees will not be happy over the change and others may fear for their jobs. Having a plan in place for handling these possibilities before the announcement is made will reduce the risk of disgruntled employees taking negative action and help keep things running smoothly during the transition process.

Computing environment – Considerations under the computing environment will include both people and systems. Keep in mind that there are a number of questions/concerns not mentioned here that relate to the computing environment. The following items would be issues in relation to security issues.

People questions would include the following:

- How is the information technology (IT) organization structured? Are the staff centralized or de-centralized? What level of accountability are they held to? How much autonomy do IT employees have? Employees moving from a loosely controlled environment will struggle with one that is tightly ruled.
- Does security fall under the IT area? If so, is there a separate department or are specified employees responsible for security? What are the reporting relationships?
- How many contractors/consultants are currently working? Are multiple firms providing services or has the company focused on one or two providers? Have these non-employees signed non-disclosure/confidentiality statements? If non-employees have system access, but no confidentiality statements have been signed, you'll want to discuss whether it is required to go back after this type of documentation with your legal department.

System considerations would include the following:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Review a copy of the current network diagram. This will include LANs, WANs, Extranets, etc. Reviewing this information will help you to understand the existing network structure, as well as identify potential vulnerability points.
- Review both a list of networking equipment being used (Firewalls, routers, etc,) and a list of equipment (mainframe, mid-range, mini-computers, etc.). Have security standards been established and a process in place for enforcing compliance? Your network staff should be able to provide a determination of the health of system/infrastructure components.
- Is a change management process in place? Life cycle management, version control and other change control concepts help to ensure changes can be backed out, tracked for accountability, that testing and user acceptance have been done, cross platform or multi-system change integration has been coordinated, and the decommissioning of applications is tightly controlled.
- Obtain a list of software and gain an understanding of the licensing agreements in place for the company. Are they adhering to the agreement terms? What kind of asset management program is in place?
- Does the company use any type of systems monitoring tools? If so, how have they been implemented?
- What is the backup strategy?

Relationship moving forward – Before getting into the details of security issues, it is a good idea to have an understanding of what the strategy is for the new acquisition. Will the acquired company operate autonomously and have minimal connections to the parent company network? Are there plans to integrate the companies more tightly together? Will the company be totally absorbed into the parent company? The plans for the relationship moving forward will have an impact on how systems are integrated and the security around them. If the strategy calls for limited connections initially and with tighter integration later on, it may not be necessary to make changes in processes initially. However, it is a good idea to lay out the requirements for tighter integration if they are different then the initial loosely coupled setup. This way the acquired company knows what to expect and can plan appropriately. Small companies that are initially allowed a great deal of autonomy will resist changes down the road if the requirements for tighter integration are not shared up front. Keep in mind that the parent company's configuration may not be the best solution for the acquisition or even the best long-term solution for either company. Understanding the strategy and planning appropriately will save hours of time in the long run.

Security Issues

The main areas of concern from a security viewpoint include the following:

Physical Security
Technical Security
Disaster Recovery
Policy and Awareness

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A sample list of specific security questions that should be answered in order to determine what issues will need to be resolved as been included as Appendix A.

Physical Security – This area is concerned with the security of the people and equipment used by the company. Physical access requirements vary depending on the nature of the business, the systems involved, type of work done on the particular platform and how critical or confidential the information is considered. Questions here will range from how publicly accessible the building employees work in to the access controls surrounding mainframe or server facilities. People who are not employees may have access to buildings in one way or another. Threats include theft, damage and copying. Sensitive information, if not securely disposed of, could yield valuable material. Other physical threats include laptop theft, natural disasters and loss of media during transport. From a systems view, the physical security is as important as the technical controls implemented. If an unauthorized person has physical access to a system they may be able to do everything from access information to removing a key piece of equipment.

Technical Security – From a technical security standpoint there is a wide range of issues to cover. You will need to understand the access controls in place; the type of data communication connections implemented; whether external entities are connected to the company systems and if so, how; are there EDI arrangements established; do any remote access capabilities exist and how are they managed, does this company Internet access and how; do they have an Internet site and do they manage it themselves or outsource; is there a firewall in place, what about anti-virus capabilities; encryption; and the list goes on. If both companies have done their homework and documented all technologies in place and the standards for using them, the easier it will be to see where there are gaps that need to be addressed as they merge together. See appendix A for an example list of the types of technical questions that you will want to consider during the due diligence process.

Disaster Recovery – Being able to recover critical systems and information is important to every company. To be successful the business must establish a plan and test it periodically. A review of disaster recovery plan and backup processes will help determine how quickly the business can be back up and running in the event of a major outage. Be certain to check how often information is backed up, as well as how the tapes are maintained, this should provide a clear understanding of how well the data is protected.

Policy and Awareness - A security policy defines the rules that regulate how an organization manages and protects its information and computing resources to achieve security objectives. A look at the acquired company's policies will tell you how serious they are about protecting data and how employee day-to-day activities impact the information assets of the company. Security policies/standards provide the framework for managing risk within an organization. They should be kept current and used as part of the audit process to determine the health of corporate information. Awareness is the means with which a business communicates the policies, standards and procedures to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

employees. Some companies make the error of not considering awareness important, however it is one of the proactive steps that can be taken to mitigate risk. Ongoing awareness of policies and risks is critical to ensuring security is kept in front of employees. An acquired company that has an active security awareness program in place will typically be interested in hearing what the parent company is doing to protect corporate assets.

Identifying the Security Gaps

Now you have the background material and the response to the security questions. The deal is done and it's time to determine what gaps exist and make plans for addressing them.

Take the answers to the questions asked and compare them to the parent company's configuration. A quick review should give you some insight to the philosophy of how the acquired company views both technology and security. Taking the background information into configuration – where are the differences and what are changes required? Prioritize the differences into things that must change within the next 6 months, the next year and so on. There may be differences that will not need to be addressed or the acquired company may have a slick system that the parent company will want to incorporate into their culture. Putting together a project plan for changes at both companies will help to establish timing. The security piece may have it's own project plan or security may tie into multiple phases of the overall plan for integration.

You may work for a company that has a 'prepare to be assimilated' philosophy, in which case it may not be necessary to spend as much time going through the steps of gathering background. However, in my experience, the time spent on due diligence for security aspects has never been wasted. Having been through the acquisition process both with and without a checklist, I can definitely state that transitions were smoother when a checklist was used.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix A
Sample Security Questions for Merger/Acquisition Due Diligence

Physical Security

- Are all areas of the building(s) freely accessible to the public? If not, describe the controls in place to limit access.
- Are computing facilities, such as rooms containing mainframe, servers, network or telecommunications equipment, etc. access controlled? If so, describe the controls in place to limit access and if an audit trail exists.
- Is after hours access controlled and logged?

Technical Security

Workstations:

- Do employees share workstations?
- Are workstations protected against unauthorized access?
- How are unattended workstations secured?

Describe the password philosophy:

- Are passwords forced to change periodically, if so what is expiration timing
- Are minimum password lengths enforced, if so what is the minimum
- Do users share IDs/passwords? If so describe the circumstances where this is allowed.
- Who administrates password resets?
- How are users authenticated prior to a password reset?

Data Communications:

- What type of systems connectivity is used between locations? (Frame relay, Internet, etc.)

Remote access capabilities:

- Are modems attached to the network? If so, who is authorized to connect a modem? For what purposes?
- Where are modems located?
- Is all dial-in activity centralized?
- Who administers remote access solutions?
- What system is used?
- Is 2-factor authentication required (i.e. smartcard)
- Is a VPN in place? If so, what applications is it used for and by whom?
- List dial-out capabilities and the controls around use.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

External Connectivity:

- Is connectivity provided to external entities?
- To who and for what purpose?
- Do non-employees sign confidentiality agreements? Obtain a sample of each type used.
- Who manages the equipment for external connectivity?
- Are non-employees allowed to dial-in to the network?

Electronic Data Interchange (EDI)

- To what extent is EDI and/or and Value Added Network (VAN) used?
- What controls are in place?
- How are connections/processes logged or monitored?

Internet:

- Is there a connection to the Internet? If so, what method?
- Do all employees have access to external networks (Internet access) from their desktops?
- What restrictions exist around Internet access?
- Are activity/access logs generated for Internet use? Obtain copies.

Firewall:

- Is a firewall(s) in place? If so, what type?
- Who manages the connection(s)?
- What services are allowed through the firewall?
- Are intrusion detection systems used? If so, which ones?

Internet web site:

- Does the company have an Internet web site?
- Are there any web servers within the network? If so, who administers them?
- What are the domain names?
- Are the sites managed in-house, or is management outsourced?

Anti-virus capabilities:

- Is any anti-virus software in use? If so, what product(s)
- Who manages the anti-virus process?
- How often is the software and definitions updated?
- Where do anti-virus solutions exist? (hard drives, servers, e-mail attachments, etc)

Encryption:

- Is encryption used?
- In what systems and for what purposes?
- What type of encryption?

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Penetration tests

- Have penetration tests or other 3rd party review(s) taken place within the last year? If so, obtain a copy. If not, you may wish to require one prior to hooking the new system into the corporate network.

Incident Handling

- Has a Company Incident Response Team (CIRT) been established?
- Are procedures in place documenting handling of specific incidents?

Security Applications

- What mainframe security system (if any) is used? RACF? Top Secret? ACF2?
- How is access control managed on servers
- Is an ESM in place?

Policy

- Do information protection/security policies exist?
- How are exceptions to policy handled?
- Is there a data classification standard in place?
- Does an information protection/security department exist?
- How many personnel are in this department?
- Is security administration centralized or decentralized? If decentralized, how are reporting relationships handled?
- Are any confidentiality or non-disclosure arrangements in place with any or all employees? Obtain copies.
- Is monitoring in place? What system(s) are used?

Disaster Recovery/Backup Procedures

- Identify types of data backup maintained (microfilm, microfiche, digital audio tapes, magnetic tapes, CD-ROM)
- Where are backups stored?
- How long are backups kept?
- Review disaster recovery plans (Have the plans been tested?)
- Offsite record storage
- Hot-site for processing
- Contracts for equipment and software. Are these agreements transferable?
- What third parties are contracted with/involved in disaster recovery solutions for the following:
  - Offsite record storage
  - Hot-site for processing
- Contracts for equipment and software. Are these agreements transferable?
- Are there legal/governmental requirements for retention? If so, is your company in compliance?
- Identify the adequacy of controls over program and systems maintenance

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References

"Information Security Risk Analysis" by Thomas R. Peltier

"30 Minute Risk Analysis" D.G. (Dan) Erwin presentation

"Joint Venture or Out-Sourcing/Contractor Scenario" D.G. (Dan) Erwin paper

"An Overview of Corporate Information Security" by Seán Boran
http://securityportal.com/cover/coverstory19991213.html#. Information domains

"The New CSO Priorities Hit List" compilation from CISSP study guides
http://www.cccure.org/Documents/JOB_TASKS/The_New_CSO.pdf

"Improving the Security of Networked Systems" by Julia Allen, Christopher Alberts, Sandi Behrens, Barbara Laswell, and William Wilson (Networked Systems Survivability Program, Software Engineering Institute, Carnegie Mellon University)
http://www.stsc.hill.af.mil/crosstalk/2000/oct/allen.asp

"CERT® Security Improvement Modules"
http://www.cert.org/security-improvement/practices/p090.html

"TRUSTe Guidelines on Personally Identifiable Information Uses in Mergers, Acquisitions, Bankruptcies, Closures, and Dissolutions of Web Sites"
http://www.truste.org/programs/mabs.doc

"Slow it down" by John Frazier
http://www.infosecuritymag.com/articles/november00/covern.shtml

"Managing the Threat Within" by Eric Shaw, Jerrold Post AND Keven Ruby
http://www.infosecuritymag.com/articles/july00/features2.shtml

"Top 10 Security Mistakes" by Alan S. Horowitz
http://www.computerworld.com/itresources/rcstory/0,4167,KEY73_STO61986,00.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 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