Global Information Assurance Certification Paper

Steps to Integrating a Small Independent Network into a Global Corporate Network

SANS GSEC Practical 1.4b
Option 1

John Belanger
January 22, 2003

This paper is a study showing the necessary steps involved in taking a small business network connected to the Internet and integrating it into a global corporate network. This became necessary after our small company was purchased by a global, multi-billion dollar corporation.

I will be discussing the various parts of the project, including the initial risk assessment, developing a security plan, integrating with the new corporate security policies, evaluating existing hardware and software, equipment configurations and personnel issues involved. As with any network, security is an ongoing issue, but this will take us up to our minimum acceptable security standards.

Background

Our small company (which I will refer to as "Little Company") develops web-based CRM software for a segment of the retail industry. The company has been in the software development business for about 4 years. During this time a small, relatively successful client-base had been established. A good portion of the development and support of the product came from an offshore office in Asia. The offshore office was using Microsoft PPTP to establish VPN connections to Little Company as needed.

About this time, a large player ("Big Company") in this segment of the industry was looking to develop CRM software itself. This $6 billion company already had sales of various hardware and software services in over 75% of the market in the United States, with a strong presence in Canada, Europe, and South America. They were looking to fill a void in their software offerings with a product similar to what we were already developing. Hence, a strategic partnership was formed, during which time Little Company had VPN access to limited resources in Big Company. After about a year and a half, the strategic partnership turned into a merger, with Big Company purchasing Little Company outright, along with the offshore office.

At this time the VPN access would turn into full WAN access for Little Company and hardware VPN access for the offshore office. The offshore office would connect to the corporate office instead of our local office. This is when security had to be re-evaluated for integration into the corporate WAN, both from the perspective of our local network and the offshore network.

One thing I should point out here is that there was no mandate from Big Company to go through these steps prior to connecting to their network. I took it upon myself to go through this process, driven mainly by what I had learned in my SANS training class. This also meant there was very little guidance from Big Company, or Little Company for that matter, due to the fact that I am the sole IT person at Little Company. Much of this process was also followed at the offshore office, whose network I oversee in addition to our local network.

The following outline was used as a guide during the process. I will explain the process we followed and pitfalls that were encountered along the way.

Outline

1. Identify key business objectives
    a. Identify the most critical business assets
    b. Identify the reason for protecting those assets
2. Identify the security objectives
    a. Identify new enterprise strategy
    b. Identify commitment to that strategy
    c. Identify who enforces and is accountable for that strategy
3. Identify and quantify areas of security risk
    a. Identify real risks
    b. Prioritize identified risks
    c. Confidentiality, Integrity, Availability
        i. What is the impact of system being unavailable?
        ii. What is the impact of corrupt/missing information?
        iii. What is the impact of unauthorized distribution of information?
    d. Impact and Evidence
        i. What criteria indicate a problem exists?
        ii. What would happen if problem never went away?
        iii. How would you measure success?
        iv. What is the ultimate goal if solution works?
4. Identify and evaluate current security measures
    a. Conduct gap analysis to determine most critical items
    b. Identify key business processes
    c. Identify administration model
    d. Identify user population
    e. Identify information architecture
    f. Identify technology architecture
    g. Identify IT and corporate standards
5. Build solutions to close gap areas
    a. Design solutions to mitigate, eliminate or manage risk
    b. Prioritize by how critical the gap and time to complete
6. Monitor and review
    a. Ensure solutions remain effective and current

Some of the documents I found helpful in starting out were RFC2196[1], and the Site Security Handbook[2] from Aquila Group which expands on that.

Identify key business objectives

> *In business be as able as you can, but do not be cunning; cunning is the dark sanctuary of incapacity.*
> ***Philip Dormer Stanhope, 4th Earl Chesterfield (1694–1773)***

The first step in establishing security was to identify exactly what it was that needed to be protected. We needed to identify the most critical business assets. Once those were identified, we had to have good reasons for protecting those assets. This helped in the process of our gap analysis that would be done later.

Determining that list of assets required the help of multiple people. Information was gathered from several departments that had different functions. I tried to get as much of a cross-section of users as possible to determine exactly what was needed. Since we are such a small company, much of this information was gathered through informal conversations, and I already had a good idea of what was considered important.

The major assets that were incorporated into the list included:

- **Web presence** – We had not only our corporate presence, which would be going away eventually, but we also had access to demo software and beta sites.
- **Source code** – This was obviously very important. With an offshore office doing development, the source code was shared between both locations.
- **Client access** – A majority of the maintenance and support was done both from the offshore office and our local office. This meant both offices needed to communicate with all client sites at all times. Any inability to reach a client server potentially meant more downtime for the client.
- **Remote access** – Since a large number of people either worked off-site or traveled frequently, remote access was an important piece to consider.

Identify the security objectives

> *We have to distrust each other. It is our only defence against betrayal.*
> ***Tennessee Williams (1914–1983)***

Once the assets were identified, it was time to identify the security objectives. What was the ultimate goal in protecting the business assets? How did that fit in with the overall corporate enterprise strategy?

The ultimate goal, from a broad view, was to make sure authorized users had access to what they needed, with unauthorized users not having access. The general public should have access only to the informational corporate web site. Only authorized users, partners and certain clients would have access to the beta and demo software sites. Only certain software developers within the organization would have access to certain parts of the source code. Very few

people would have authorized access to everything. We also had to be sure that in the course of connecting to client servers that the clients themselves could not connect back to our network.

As stated earlier, there was no mandate from Big Company to follow any certain strategy. It was up to the local office to decide what technology was to be used and how the business assets were to be protected. I did manage to dig up some policies that Big Company had in place, and decided to use those as a guideline. Other helpful tools were security recommendation guides from the NSA[3]. These covered general network issues as well as operating system-specific issues.

Given that there was no mandate, this meant the commitment to our new strategy would have to come from the local office. That also meant any enforcement of that strategy would come from the local IT department (me) and local management. Everyone would be accountable for the strategy at some level. The users would be accountable for their own actions, such as loading unauthorized software, contracting viruses from non-company email accounts, etc. The IT department was accountable from the network side of things, making sure the network configurations were correct, anti-virus software was up to date, monitoring installed software, etc. Local management was accountable for making sure everyone was aware of the policies.

Identify and quantify areas of security risk[4]

> *In cases of defense 'tis best to weigh the enemy more mighty than he seems.*
> ***William Shakespeare (1564-1616)***

The next step was to look at our list of assets and the current network configurations, and identify and quantify the areas of security risk. The hardest part was identifying exactly what those risks were. We already had a good idea of what some of our at-risk areas were. A logical starting point was the SANS/FBI Top 20 List[5]. This list describes the most common vulnerabilities for Windows and UNIX systems. It includes what the problems are and how you can protect against them. Another good resource is an article by Charl Van der Walt on what risk assessment really is[6].

You also have to view end users as a security risk[7]. End users themselves may be the risk. There's always at least one user who knows just enough to be dangerous. They may also be susceptible to social engineering.

Once we had a list of our security risks, we had to prioritize those risks. While there was risk on many levels, we gave priority to those risks which directly impacted the security objectives. Other security risks could be dealt with at a later time.

Next was to compare these risks against the three bedrock principles of security: confidentiality, integrity and availability[8].

What is the impact of each part of the system being unavailable? Our corporate web site is purely informational, and somewhat out of date. If that were unavailable for a period of time, there would be little impact on the business. On the other hand, if we lost connectivity to our clients, it would be impossible to perform the daily maintenance routines and respond to support calls.

What is the impact of corrupt or missing information? If our source code version control software became corrupt or source code was missing, that would have a negative impact on productivity. Many hours could potentially be lost restoring previous versions from backups. This would also cause problems if the corrupt source code was not caught before applications were deployed to client servers.

What is the impact of unauthorized distribution of information? If the source code was somehow compromised, there would potentially be disastrous effects across all clients and their networks. Theoretically someone could insert malicious modules to do just about anything, from simple annoyances of defacing web pages to distributing Trojan applications. Anything along those lines would lose any credibility we had with clients. Protection of the source code was of vital importance.

Another decision is to determine what criteria indicate a problem actually exists. Do you look through logs to determine if someone has tried gaining access to the system? Has someone gained unauthorized access in the past? Have you done any sort of penetration testing on your own network? Once these problems have been identified, what would happen if these problems never went away? How would it impact the business?

For instance, say you did your own penetration testing. The results show that you have an exposed FTP server. Further, the banner headings show that the version of FTP server running is an older version, with many known vulnerabilities and perhaps a default installation. Depending on where this service is running, it may not pose much of a threat to your network. On the other hand, if it's running on your Windows domain controller (for the sake of argument), there is the potential for a hacker to gain access to user account information. In this case, you may want to move the FTP service to another machine, or at least make sure all the patches are installed and up-to-date.

Many tools are freely available to perform your own basic penetration testing. There are several papers in the SANS Reading Room which describe various ways to assess your internal security. Timothy Layton writes a good paper describing penetration testing and the tools you can use[9]. Below is a partial sample from running fscan, a port scanning tool from Foundstone[10].

```
Using 64 threads.
```

```
 Connect timeout set to 2000 ms.
 Ping timeout set to 2000 ms.
 Scan delay set to 0 ms.
 Appending to output file.
 Banner grabbing enabled.
 Quiet mode selected. No pings.

 Scan started at Thu Nov 07 14:47:24 2002
.
.
.
Scanning TCP ports on 127.0.0.10
127.0.0.10      7/tcp
  ....
127.0.0.10     13/tcp
  2:23:14 AM 11/8/2002.
127.0.0.10     17/tcp
  "The secret of being miserable is to have leisure to bother about whether.
  . you are happy or not.  The cure for it is occupation.".. George Bernard
  Shaw (1856-1950)..
127.0.0.10     19/tcp
   !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg..
  !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh..
  "#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi..
  #$%&'()*+,-./0123456789:;<=>?@ABCD
127.0.0.10     21/tcp
  220 raju Microsoft FTP Service (Version 5.0)...
127.0.0.10      9/tcp
127.0.0.10     25/tcp
127.0.0.10     42/tcp
127.0.0.10     80/tcp
  ..<html><head><meta http-equiv="Content-Type" content="text/html; charset=
  english"><title>HELLO!</title></head><bady><hr size=5><font color="red"><p
   align="center">Welcome to http://www.worm.com !<br><br>Hacked By Chinese!
  </font></hr></bady></html>
127.0.0.10     53/tcp
127.0.0.10    119/tcp
  200 NNTP Service 5.00.0984 Version: 5.0.2159.1 Posting Allowed ..
127.0.0.10    139/tcp
  .....
127.0.0.10    135/tcp
127.0.0.10    445/tcp
127.0.0.10    563/tcp
.
.
.
Scan finished at Thu Oct 03 16:06:42 2002
 Time taken: 152386 ports in 4757.563 secs (32.03 ports/sec)
```

You will notice that the results from the web service on port 80 indicate a problem. This is not something that you want to see on a production system.

Once you have decided that problems exist and what the risks are, how do you measure the success of eliminating those problems? What is the ultimate goal if your solution works? It may be something as simple as performing another penetration test on your network after your solutions are in place. In the previous example, maybe the solution is to completely disable the FTP service that you discovered. Problem solved. If you really need that FTP service, though, a better

solution may be to dedicate a machine to FTP services, perhaps a machine that is not part of your corporate domain, or better yet not on the same network as your critical servers. The goal here is to provide FTP services to users that need it, while reducing the risks of unauthorized users gaining access to systems through this service.

Identify and evaluate current security measures

> *What boots it at one gate to make defence, And at another to let in the foe?*
> ***John Milton (1608–1674)***

Perhaps one of the easier steps in this whole process is to identify and evaluate your current security measures, or at least what you think you have. This, of course, depends on the size of your system and how familiar you are with it. Since ours is fairly small and I have been here a few years, I was very familiar with it. Still, a gap analysis was performed to determine what we currently had and what was needed to get to where we wanted to go. The following areas were used to evaluate our current measures and controls:

Business processes – Authentication, access controls, critical applications
Determine what the critical applications are that users need, and how they access them. Are simple username/passwords enough, or are stronger credentials needed, such as Smartcards or fingerprint scanners?

Administration model – IT staff location, delegation of IT functions
Being a small company, this was fairly straightforward. All administration was done from a central location, and all functions were done by a single person, along with a designated backup when needed.

User population – user requirements, department requirements, user profiles
Determine what requirements users may have, such as access to certain web sites, the ability to establish a VPN with a vendor, etc. Do only certain users have those requirements, or entire departments?

Information architecture – data workflow, repository locations
Determine what the current data workflow is, and whether it can or should be modified. Determine locations of the important data, such as a central file server, source control server, etc.

Technology architecture – physical and logical topology, security infrastructure
Determine and draw out the current physical and logical topology of the network. It is an immense help to visualize how everything is connected, and the relationship between devices. It will also help determine how your security is currently configured, and whether or not you will need additional devices.

IT and other standards – security policies, IT policies, organizational policies

Determine what your current security, IT and organizational policies may be. Do you currently adhere to those standards? Do you currently have standards? If not, now is a good time to get those in place. A good place to start would be the SANS Security Policy Project[11]. You'll find many tips and hints regarding policies, standards and guidelines, along with examples and templates.

Build solutions to close gap areas

Better be despised for too anxious apprehensions, than ruined by too confident security.
Edmund Burke (1729 - 1797)

Now that you know what you have and where you want to go, you can begin to build solutions to close your gap areas. You need to decide on an appropriate action for each risk item. Your solution should mitigate, eliminate or manage the corresponding risk.

Elimination is the ideal solution. This is where you get rid of any risk that you may have had on a permanent basis. This is not always possible.

Mitigation is when you cannot totally get rid of a problem, either due to economic or technological reasons. Mitigation helps reduce the risk to an acceptable level.

Managing a risk is what you do if you can not either eliminate or mitigate the risk.

The solutions you come up with must also be prioritized by how critical the gap is along with how long it will take to complete the solution. If there is minimal risk and the solution will take many weeks and thousands of dollars to complete, that particular solution will move down the list of priorities. However, if there is a critical solution that is fairly quick and easy to implement, that will move towards the top of the list.

There are two formulas you can use to determine your risk factor for single occurrences and annual occurrences, SLE (Single Loss Expectancy) and ALE (Annualized Loss Expectancy)[12].

SLE (Asset Value) x (Exposure Factor) = Single Loss Expectancy	$1.5 million x 50% (0 – 100% of loss to asset) = $750,000 (loss expectancy due to improper security)
ALE (Asset Value) x (Exposure Factor) x (Annualized Rate of Occurrence) = Annualized Loss Expectancy	$1.5 million x 10% (likelihood of breach without proper security) x 5 (estimated annual rate of occurrence) = $750,000 (loss expectancy due to improper security)

Monitor and review

> *The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved.*
> ***Confucius (551 BC - 479 BC)***

As with all security solutions, things are constantly changing. Effective solutions must be managed and reviewed to ensure that things are up to date and keep pace with any network changes, newly discovered vulnerabilities, and new policy changes. Systems must be kept up to date with new patches and service packs. Occasionally review your system logs and do your own penetration testing to make sure things are going how you think they should be.

Don't rely on a single security method. Simply installing a router with firewall capabilities is not a complete solution. Deploy multiple security measures to thwart possibilities of attack.

Conclusion

These are the basic steps that were followed for our particular network. Since the merger was fairly recent, many of these steps are constantly being re-evaluated. The key is to have a plan and stick with it. New vulnerabilities are always being found, new patches being released, and new technology being developed both to help and hurt the system administrator's cause.

References

[1] Fraser, B. RFC2196 URL: http://www.ietf.org/rfc/rfc2196.txt (22 January 2003).

[2] Canberra Aquila, Inc. URL: http://www.aquilagroup.com/pdf/site_security_handbook.pdf (22 January 2003).

[3] National Security Agency "Security Recommendation Guides." URL: http://www.nsa.gov/snac/index.html (22 January 2003).

[4] SANS Institute. SANS Security Essentials III: Internet Security Technologies. Part 6 Risk Management.

[5] SANS/FBI Top 20 URL: http://www.sans.org/top20 (22 January 2003).

[6] Van der Walt, Charl. "Assessing Internet Security Risk, Part One: What is Risk Assessment?" URL: http://online.securityfocus.com/infocus/1591 (22 January 2003).

[7] Conry-Murray, Andrew. "Securing End Users from Attack." Network Magazine October 2002 (2002): 28-32.

[8] SANS Institute. SANS Security Essentials II: Network Security Overview. Part 1 Defense in Depth.

[9] Layton, Timothy. "Penetration Studies – A Technical Overview." 30 May 2002. URL: http://www.sans.org/rr/penetration/studies.php (22 January 2003).

[10] Foundstone, Inc. URL: http://www.foundstone.com/knowledge/free_tools.html (22 January 2003).

[11] SANS Institute. "The SANS Security Policy Project." URL: http://www.sans.org/resources/policies/

[12] SANS Institute. Security Essentials III: Internet Security Technologies. Part 6 Risk Management.