Global Information Assurance Certification Paper

The Pursuit of *Defense in Depth:* Balancing Information Security and Business Practices

Nate Duzenberry

January 28, 2002

Summary

The topic of this paper is the Pursuit of *Defense in Depth*. I have chosen to focus on four key areas within this overall topic. I want to start by looking at:

- Simply trying to define the phrase of *Defense in Depth*
- The challenges presented in trying to achieve *Defense in Depth*
- The aspects of setting realistic expectations for you and your company as you seek this goal
- The bottom line of balancing the costs with the results

In this process, I will be making several assumptions and I will speak of several typical scenarios as I try to avoid direct references to my current or previous environments.

Lets start at the beginning and try to walk through these issues. To simplify the discussion, I am assuming that everyone has some mix of the following components in their network. We will see them vary in size, use, and nature, but we all typically have Internet and/or Extranet connections, a perimeter router and/or firewall with/without a VPN, and some variation of a WAN/LAN. When practicing Information Security within our networks we gain technical challenges in areas such as Network Penetration Testing, the before mentioned Firewall/VPN (Virtual Private Network), NID (Network Intrusion Detection), and HID (Host based Intrusion Detection). We also need to consider the areas of Vulnerability Assessment, Security Policy Management tools (example: Axent ESM), Audit Reporting tools (example: HP ITO), and this is without even touching the areas of Corporate Security Policy or the related System Technical Policies.

If these are not enough topics, I am sure we can find a few more to add, or we can simply elaborate on the very brief areas already mentioned. The categories I listed are the proverbial ‘tip of the iceberg’. I am enclosing information on an easy to use glossary available on the Cisco web site to help in defining any of the above network terms (see the references below). Please keep in mind that I have only provided a very simplistic view of the network areas, and each technical area can easily be broken down into a larger listing. Lets move on to the real topic and try to define *Defense in Depth*.

Defining *Defense in Depth*

The phrase *Defense in Depth* is an interesting one. The first time that I heard it was during my SANS GIAC course. I have since came to appreciate the phrase and have found myself using it a lot in my career. The best example I have found to explain *Defense in Depth* is taken from the GSEC course as part of the Information Assurance Foundations class. Stephen Northcutt of SANS.org describes it as meaning, "One layer of defense is just not enough. It is to protect (secure the systems to the extent possible), Detect (learn to detect and analyze the attacks directed against my organization), react (strengthen the defenses based on the analysis of the attack). **Protect, Detect, and React.**" I have not been able to find a better example that can drive these points home.

In my previous life the phrase ‘due diligence’ was of our unit of measurement. This was within the realm of a government contractor where the phrase had more of the common government GAO (General Accounting Office) meaning. While this phrase shares a similar meaning with *Defense in Depth*, I believe that the examples I provide in this paper will illustrate the subtle differences. For anyone who is unfamiliar with the phrase, due means expected or scheduled, and diligence means earnest and persistent application to an undertaking; steady effort; assiduity, or attentive care. That is at least the Webster’s definition. When we put that into context with its GAO use, it gains the layman’s meaning of "meet our guidelines, or pay a fine." While this can be a nice environment at times, it, at least in my experience, has often fallen short of *Defense in Depth*. The GAO like many government agencies is plagued with outdated guidelines and enough bureaucratic red tape to mummify us all.

Introduction and Personal History

I would like to welcome you to the never-ending madness! I believe that it takes a certain character to really enjoy this field. I am going share with you some brief personal information and history to provide two different example environments. The two environments vary widely in content and implementation as one could really consider them to be separate schools of thought. One environment focuses on confidentiality and protection of patient information for

compliance with HIPAA (The Health Insurance Portability and Accountability Act of 1996), and the other focuses on protection of customer information in a Banking and Financial Services environment for compliance with the GLBA (Gramm-Leach-Bliley Act).

I am a fairly young, yet hopefully somewhat seasoned, practitioner of Information Security. I have been working for a large bank for almost 2 years. I gained most of my experience in the field while working as a government contractor for the DOD and Health Care Finance Administration. I decided to leave behind my government glory days and test the corporate waters. You will find that my story is probably not a new one and my problems are fairly typical within most enterprises.

Example A: The Financial Services and Banking environment

In the past year alone, we have been witness to the passing implementation date for compliance with the GLBA. This act, also known as the Financial Services and Modernization Act (FMA99), is intended to revolutionize how financial institutions ensure the security and confidentiality of customer information. One of the most simplistic and useful resources that I have found detailing this act is a white paper provided by ICSA TruSecure (see the URL below). I am one of the fortunate few that work for a financial institution that has adopted a proactive approach on compliance with this act. My organization has dedicated resources within our legal department to provide a simplified listing of the potential impacts of the Act. I cannot share our actual document with you but for a simplistic explanation the TruSecure white paper details the specific actions that financial institutions must take.

This is only one particular concern or task that has been sitting on our plates lately. The overall purpose of my group is to provide security planning and consulting services to the corporation. This can at times be a daunting tasks simply based off the shear size of the company. Also we are faced with the typical challenges of a large bureaucratic structure where streamlined processes that were intended to be nimble actually handle more like a school bus.

Example B: The life of a Government contractor

I could never claim that I was bored. During my time with these groups, I witnessed and worked with many interesting things. I actually had the pleasure of watching the Health Care Finance Administration implement many of its HIPAA policies. Needless to say a large environment with many diverse systems. I got a crash course in everything from AIX, Oracle, Netscape IPlanet/Directory Server, NID/HID, lots of NT, and the list continues. It is humorous to think back and know that a person such as myself, with mainly NT, a little Unix, and a little Cisco experience could at that time suddenly become a firewall administrator.

I was fortunate enough to work with a great group of diverse people all thrown together and yet linked by the same common goals. (In the end, I think that we meshed together to make a pretty good batch of chili). In all seriousness, we had contractors from all specialties involved in Network, Database, Application, and Security Engineering of systems related to Medicare and Medicaid. This was one of those open job experiences where I was free to work on anything that I was willing to be responsible for. I was also fortunate enough to gain exposure to the USPS NetPost and HCFA Constructive Key Management implementations. For a person that was just starting to get a grip on Certificate Authority policies and some 220 SSL key pairs this was a mind blowing experience.

Needless to say, we were busy. The documentation to support our work was always outdated or non-existent and the cleanup effort on the back end to document all systems to meet GAO, HCFA, and HIPAA requirements probably continues today.

Challenges Presented in Trying to Achieve *Defense in Depth*

I may have a bit of an unorthodox approach but I admit that I am not the best planner. In all of my previous experience, I could try to produce 10 documented plans for an implementation and I would always wind up with stacks of paper on the floor and chicken scratch notes on each page. I would always find some large detail that I had missed or a reason to deviate from the original path. After several attempts and lots of frustration I decided to try to keep it simple and do only what I had to. This approach has caused me a few problems over the years and is not recommended for everyone.

My current philosophy is "lets try to keep it simple." I like to try to focus on one particular problem at a time. This is not always possible and also means that you will have to prioritize your work and decide which problem to conquer first. It always helps me to to walk through the problem and any potential resolutions. I consider this my version of a "from the ground up" approach. I have learned that I need to understand and thoroughly define the problem before I start to work on it. This itself can be a large challenge in your project and your overall goal of *Defense in Depth*.

(The following is a hypothetical situation; I hope that it will provide an example of why you need to know your problem before you design the solution.) Lets say that HCFA came to us and discussed the need to secure the fifty plus servers they have located at each state location. This is a complex request with several potential solutions. We now need to understand their problems and needs so that we can then decide how to handle this request. Do they simply need a report or log to satisfy an audit requirement or are they concerned about system vulnerabilities and exposure, or possibly both. This is only a few of the questions we would need to answer in order to define our security solution.

Lets add some more information to this example to make it a little more realistic. Your manager is a decent straightforward person but he is not the most technically savvy. He has been given the task of coordinating communication between HCFA (the business unit in this case), and the group of engineers. He communicates to you that HCFA is interested in securing these systems and (from memories of your prior discussions with HCFA staff) you assume that they mean the ever-lingering need to implement a firewall. This is the source of a monumental mistake. If I can stress anything in this paper, it is do not make assumptions. You can probably guess what happens next, my assumption was wrong. As a result of my assumption, my company reacts with a huge effort and produces formal proposals to implement some fifty firewalls at each state location. These proposals include everything from a cost analysis of three leading vendors to potential configurations, theoretical implementation dates, and a network impact analysis. You can easily wind up wasting months.

The proposals wound up being the cause for a lot of internal debate as certain factions start to question why they need more firewalls. Suddenly someone bothers to communicate the fact that they were more interested in satisfying an audit-reporting requirement. This now winds up becoming a hot topic, where because of an assumption and miscommunication, you have wasted your time and resources. You now only have a month to implement a solution for security log harvesting to meet an audit requirement. This situation could even potentially have the need for some type of Host based Intrusion detection and centralized log collection. You now get to have fun running around like a chicken to piece mail together a solution for log harvesting. Further down the road you decide to tie in a (HID) implementation. This is where the never-ending madness can come into play.

In the end, rest assured, things normally always have a unique way of coming full circle. That well-crafted firewall proposal has been collecting dust on some CIO or CTO's desk. Sometimes they actually brush off the dust and think that your proposal is still valid, they may even want to implement it with next year's budget. In my previous dealings, and using the government as my example, I have seen stranger things occur.

The whole purpose of my previous example is to communicate the human or social related challenges in Information Security. Communication can be paramount. Know your problem well, get it defined and your tasks agreed on before you start the work. You will need a list of the desired results, you will also want to keep a list of the problems you encounter, don't forget about version control or disaster recovery in the process because no one seems to appreciate a design that is hell to support. There are many more items that we could list and this is why you have to break apart the problem into workable pieces, you may choke otherwise. This is where I started to understand the need for simple step-by-step approach. When you look at a problem and decide how to tackle it, you may wind up with several related projects. You will need to define a scope (beginning and end) for your projects or your managers will begin to think that you never get your work done. You do not want to be caught in the quick sand of a never-ending project; it can have ill affects on your career.

I feel that the challenges you will face as you seek your goal of *Defense in Depth* can be split into four key business related areas. They are Communication, Project Management, Information Technology related, and Political or Business. This is simply my opinion and I am sure that others can find several other potential groupings. This is simply the way that I try to again keep it simple. I believe that I have already provided an example of the potential communication challenges that you may experience. Now, lets see if I can provide some brief examples for the other areas.

Project Management is a skill that is in my opinion comparable to organization skills. If you were a neat kid in school and your desk did not look like a hurricane developed inside of it, you were always on time and had your homework done, then you might actually be good at this sort of thing. I seem to quickly lose patience for it as so many of my projects have seemed to become bogged down in departmental politics. I hope that your experiences will be better than mine have been in this area.

Information Technology related areas might comprise a vast portion of your project dependent on what you are actually dealing with. This may be anything from a new technology to a large implementation of an existing one. I mentioned previously that you would not want to forget about configuration management or disaster recovery efforts. I normally group these items in with their related technologies.

Last but not least, we have the Political and Business related categories. While I have little patience for these areas,

it does not make them any less important. The overall importance to at least maintain a cordial relationship with the political powers in your environment is imperative. You will never know when you will need them as your allies and without a decent channel of communication, you will find it impossible to deliver the details related to your project. This can affect the all-important purchasing and implementation approval process. To make a long story short, when communicating a technical issue to a non-technical group, keep it as simple as possible and try to keep it at their level. I have learned that they can quickly become frustrated when you talk over their heads and this may result in either a shortened life span for you or your project.

Although my commentary may have been somewhat long winded on the particular issue of challenges that you may face in your pursuit of *Defense in Depth*, I feel that topic by itself could serve as the sole topic for future GSEC practical assignments. I feel it is difficult to do this one justice, however I hope that the examples and commentary I have provided may serve to provide some details of my real world experiences. Parts of my commentary are vague and hypothetical to simply avoid direct references to previous environments. I have chosen to use the HCFA name specifically though, which has since changed, simply because a government example does not hold up very well without a government agency to pick on.

Aspects of Setting Realistic Expectations for You and Your Company

In the SANS GSEC course, Stephen Northcutt routinely emphasizes the importance of getting your plans documented in writing and signed before you do any work. I agree and must also emphasize the importance of having documentation in place to protect you. It does not matter whether you are simply scanning the internal network for IIS boxes and vulnerabilities, or password policy compliance. Let us take this one level higher and state the importance of having your security policies published and available for almost everyone in your organization to reference. It is not usually a good idea to expose this information on the Internet. This may seem to be a obvious comment, however I have seen it done-so it is not irrelevant.

I will provide some hypothetical commercial examples of Security Policy structure. I am not in any way suggesting that this should be the structure for everyone. Most commercial environments that I have been exposed to have some form of an Information Systems General Security policy. This may be separate from the overall corporate or physical security policies. I have seen it vary widely dependent on the environment. You may need other documented policies dependent on how specific your general security policy is and how diverse your platforms may be. I personally like having specific technical policies on everything from IIS, Windows 2000, Linux, Apache, and even MVS. SANS has a mention of a personal security plan and I have found that option interesting. I wish I had thought of that idea when I was a contractor and needed some additional coverage. As I stated this is my preference and it will depend on the needs of your environment as to what the right fit is for you.

All of this will begin to make sense with its relevance to realistic expectations for you and your company once you take into account the need to establish standards. Without standards, it is very hard to define what you can and cannot do. I have found, for example, that without a standard stating that you will not have network-attached systems with modems installed that it is almost impossible to enforce. This may be the case with everything from IIS and web application to Windows 2000 Servers and Active Directory. Standards are the one thing that will help protect you from Business Units screaming that you are a Gestapo faction and impossible to deal with.

One of the items that has become the greatest source of frustration personally, is consistency. Let us use a large corporate environment as an example. I feel that the standards are pretty straightforward and not open to a lot of interpretation. The problem is apparently that I am one of the few that feels this way. If you work within a large group that provides services across the corporation, it sometimes appears that the attitude will change to what is more often good for the business rather than what is secure or follows policy. This in a sense can stand to greatly weaken or undermine the same policies you are trying to uphold and enforce. This is something new for me and very frustrating. While I understand that business needs must be taken into account I do not feel that ignoring policies or security standards should be allowed.

One business that I am aware of has adopted a whole process of risk acceptance where you may have to document the areas outside of compliance and try to quantify any risk to the business units. If the business unit does not feel that the risk is great or outweighs the cost then they get to sign off and accept the risks posed to their environment. They agree that they are responsible if anything should happen. This process would be fine if you could establish consistency within the central group that documents the risk acceptance. Lets say, for example, that your dealing with a remote access standards on a WAN. Do you let one affiliate accept the risk for what may be a potential threat to the whole WAN and all members? My answer to that is NO, and this is one item where consistency has been and will continue to be a very important issue.

One interesting question that always seems to come up-what do we have the power to say no to? In my Government

experience, we had complete control to say no to anything that we did not want. If it was something as simple as the fact that we did not like it, we could always find some reason with the tools available as to why it was either a bad idea or not secure. This seems to be a different ball game when dealing with the corporate environment.

When playing in the game of cost versus benefits many companies will ask you 'why do I need to encrypt this information?" "Why do I need this firewall", or "why can't I have a modem on my computer so that I can dial into it from home?" You should have sound stable standards documented so that you will not get overwhelmed with these questions and you can state that it is because it is against company policy. I hope that you can let the documented company policies be your security blanket. Sometimes you will still get stuck with the joy of arguing with some VP who may still not agree with you regardless of the company policy.

The Bottom Line of Balancing the Costs with the Results

At some point it all comes down to cost justification. Someone or something must convince businesses or agencies that they must protect our data in a certain manner. Luckily, we have laws such as HIPAA or the GLBA that will hopefully assist us in this endeavor. I think that we all know that there will always be companies or organizations that will not comply with these standards or listen to the industry when we discuss potential threats.

We all will have to fight our own political battles when dealing with issues of cost justification. For instance, I cannon state in my previous example the dial-up access to the WAN is not needed or beneficial. The need is obviously defined and in this case it may be something considered legacy that has existed for sometime. The affiliate may simply be measuring the cost of converting the users to the corporate VPN solution and not like what they see. That is within their right as a business unit and they may need to evaluate the impact of corporate initiatives on their environment. It then becomes our job to try to understand the bigger picture and evaluate all potential areas that may be exposed to any risk. You are now faced with the duality of empathy with the business unit and mitigation of risks posed to the corporate WAN. Unless you are high enough on the food chain, I do not try to make these judgment calls and I like to leave this to the higher political powers to debate. All that we can normally provide are the facts in accordance to the policies that we have adopted. After all the policies we implement will serve as the guidelines that we are all measured by.

We do not always have to agree with the political decisions, however I do like to see the evolving policies and ever changing environments. You will find in your practice that many people will say they have the perfect recipe for this scenario or situation and you will be convinced to try several of them. I would recommend that you remain skeptical and measure all solutions based off of performance in your environment. Always try to get information from trusted sources and do not get caught up in yet another sales pitch or branding debate. I would always encourage you to be as familiar and intimate with your environment as possible. I believe that it is hard to secure something you do not understand or cannot support.

It is my opinion in writing this paper that I do not believe anyone has a simple step-by-step solution to information security that will work for everyone. There are a lot of technologies and tools that can be implemented. There are a lot of policies that can be documented and adopted. I cannot tell you since I do not know your environment which specifics may work best for you. I think that it is more important that we all work together and share information on the basics and foundations so that we all may all learn a little and stand a little stronger.

All of these reasons combined with the environment itself are the reasons why I welcome you to the madness. I wish you the best of luck in your pursuit and wish to share these remarks of wisdom that I have come to appreciate. Take nothing for granted, expect the unexpected, set all of your conditions for protection during system failure and enjoy the times when you actually succeed. We are after all trying to beat hackers at their own game and practicing a science of obscurity when you must assume that there are ways to attack virtually any system.

References

Cisco Glossary Connection, http://www.cisco.com/warp/public/5/glossaries/logos/

Health Care Finance Administration, HIPAA http://www.hcfa.gov/hipaa/hipaahm.htm

Gramm Leach Bliley Act, GLBA http://www.senate.gov/~banking/conf/

ICSA TruSecure white paper on GLBA, http://www.trusecure.com/html/tspub/whitepapers/glb_paper.pdf

CKM reference information, TECSEC http://www.tecsec.com/SetFrame.asp?Sec=CKM1

Network Intrusion Detection or Host based Intrusion Detection reference materials for NID or Cyber Cop Monitor, http://www.ciac.org/ciac/

Security Planning Resources, http://www.sans.org or http://www.trusecure.com