Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b (Option 2)

Establishing a Business Unit (BU) Security Team

Brian F. Schutt
July, 2003

Abstract

Most large companies that implement some form of security program usually start at a corporate (high) level. These programs strive to implement the components of a solid defense in depth strategy. The hiring of personnel, the establishment and control of the corporate security policies, program management and tools development often lies with individuals and teams at the highest organization levels in these large companies. The nature of security work requires a high level of authority and power. But what about the business units that comprise a large enterprise? They require access to all of the same defense in depth structures, but they also need autonomy to operate independently according to the needs of the business unit while still adhering to policies and procedures created with the corporation in mind.

The company I work for is a large manufacturing enterprise. I work in one of the business units within one of several operating groups that comprise the company. This paper will present a case study of how our business unit formed its own security team within the context of a larger, corporate security organization. I will describe how we recognized the need to establish a security team, thanks, in part, to the Nimda and Code Red viruses, and how we addressed two main categories of security issues, the tactical and organizational. We learned the importance of addressing both categories to ensure that they comprehend the demands of the other. Finally, I will describe the state of our BU security team today in terms of the current projects, our team structure, and how we see our mission serving our business unit moving into the future.

Table of Contents

Before the Security Team was Established

Like most companies, the events of September 11, 2001 profoundly affected the way my company views security. Shortly after the attacks on the World Trade Center (WTC) in New York, our chief executive officer created the Safety and Security Initiative (SSI). He chartered the Security and Safety Task Force to review security measures at our company sites, maintain the safety of company employees worldwide, and ensure that our company's business continues uninterrupted. The effort was a two-pronged approach: secure our computing infrastructure, and reinforce and improve physical security. The latter is more tangible, and our company took steps to make structural changes in the form of concrete barriers outside some of our campus buildings, reduce access to the data center, and install portal scanners in lobbies at main company sites. The former is the main topic of this case study.

What 9/11 did for our company was to emphasize the well-established, and often neglected relationship between physical security and the logical security implicit in our computing environments. The attack on the WTC was targeted at nearly every well-accepted, standard area of physical security documented by the University of Chicago's Network Security Center. The unique and extraordinary aspect of the 9/11 attacks, as it relates to physical security, is that the attackers had no intentions of exploiting or keeping intact the systems that they were attacking. The terrorist act was designed to disable and destroy those systems, not compromise or hack them.

Prior to our company's heightened awareness of the need for and mobilization toward a more formal security program, we did have a team focused on security, but with a scope much less comprehensive than a complete defense in depth strategy. The team was a cross-functional, multi-site team made up of representatives from all the company's business units which strived towards these goals:

- Provide customers with high quality, standardized anti-virus products
- Provide customers with timely virus information
- Understand virus technology and provide expert-level support for virus issues
- Respond in an orchestrated fashion to single and multi-site virus emergencies

As you can see from the goals, these efforts were concentrated on responding to the effects of computer viruses. The team defended the common virus infection vectors: disk usage, local area networks (LANs), telecommunications, and spontaneous generation. The representatives of the business units, in most cases, used this body as their primary security team. This was the case for me and the business unit I represented.

Our company also had a group dedicated to information security at a corporate level. From a reactive point-of-view, it was this group's function to act as the computer incident response team (CIRT) for our enterprise. Proactively speaking, it was the responsibility of this group to define corporate requirements for each of the main, high-level goals of IT security: confidentiality, integrity and availability.[1] When this group was engaged, they asked the following questions to help the business units determine what their security requirements were:

1. Is a formal Security Risk Assessment required?
2. Confidentiality requirements
   - How will we control access to classified information?
   - How will those controls be checked, monitored and maintained for compliance?
   - Will users be required to perform security activities? (e.g., Authentication to confirm they are who they say they are.)
   - What intrusion detection measures will be needed?
   - What will control copying, printing, forwarding, and viewing of classified information?
   - Are there other protection requirements?
3. Integrity requirements
   - How will integrity of classified information be assured and validated?
   - What is the frequency of audits required?
4. Availability of Service requirements
   - Is Denial of Service (DOS) an issue or vulnerability?
   - How will DOS attacks be monitored and responded to?
   - How will availability of service be measured?
5. End of Life (EOL)
   - How will the system be disposed of at EOL that ensures information assets are not compromised?

There was minimal input from the business units during the requirements definition, and little consultation with members of the business units about what the effects of these requirements would have on the business units. This is the first key factor in the evolution of security teams within my and the other business units.

In addition to these formal groups, the engineers and system administrators within our business unit (and presumably others) implemented Microsoft Windows™ and Unix security on the servers under their control. This effort was informal and not codified. It followed the industry standards and practices for hardening the operating system. My company allows our business units to operate with autonomy, and this trait of our culture is highly valued. Therefore,

[1] "N2N Security Requirements Model," Page 1.

each unit is free to define their own standards and practices. This is the second key factor in the evolution of our security team.

With these two entities in place, it took real-life attacks to crystallize the need for a security team within our business unit. The first of these was the Code Red virus that struck the Internet in mid-July, 2001. The second followed closely on the heels of Code Red, and it was the Nimda virus that appeared just two months later in mid-September, 2001.

It was nothing, in particular, that these viruses did to our company that caused us to change our operating model. It was the fallout from the immediate impact to business operations and the loss of productivity from the subsequent cleanup that led us to form a security team for our business unit. The first incarnation of this team was actually seeded with members of one of several vertical organizations within our business unit and did not actually represent the entire unit yet. Their modus operandi was a "divide and conquer" approach to the reaction to and mitigation of the vulnerabilities exploited by Code Red and Nimda on the servers under their control. This approach was effective, but it still lacked a comprehensive approach to security. The engineering staff was still in a reactive mode rather than a proactive one, and they made server patching their top priority. Little attention was paid to or effort expended on prevention or detection. No effort at all was spent on prediction. The business unit still lacked a strategy to implement comprehensive defense in depth.

The managers of our business unit took some time to realize that each vertical organization within the unit would eventually form their own security team, and to avoid this, they formed a virtual team whose job it was to address computing infrastructure security for the entire unit. It was at this point that the real work of the security team began.

Establishing the Business Unit (BU) Security Team

Our BU security team was lead by a manager from our Application Security team and was comprised of representatives from each vertical organization within our business unit. We utilized all the normal business tools that facilitate a geographically dispersed team. There were two weekly meetings: one that focused on planning, and the other that focused on the status of our tactical activities. Each representative also met individually with the team manager on a weekly basis to review progress within the vertical organization. To facilitate regular communication, the team used email with distribution lists, multi-line conference calls, and a team website.

The initial stages of forming our business unit's security team was rife with uncertainty and a lack of clarity. Many questions were raised: What is the mission? What areas of security should be emphasized? Who is responsible for achieving the mission? Who's in control? How does it fit with the corporate team and their mission? We knew that something had to be done to secure our BU's computing environment, but we just weren't sure how to organize our efforts. The scope of the effort was a heated topic of debate from the outset. Another factor that complicated operation of the new team was that it included members from all geographies: the Americas, Europe and Asia.

The issues we began to wrestle with (and continue to wrestle with today) fell into two categories: **tactical** and **organizational**. This dichotomy is echoed in a recent presentation by Roberta Witty of Gartner in which she states,

> "There are two sets of distinct information security activities: the technical / operational set (security administration, firewall administration, virus detection/prevention, technical security architecture, others) and the strategic / planning / management set (policy development, IT risk management, business security architecture, implementation of new regulations, others)."[2]

What Ms. Witty refers to as the "technical/operational" activities is equivalent to what I will call the *tactical* category, and the "strategic/planning/management" activities equate to what I refer to as the *organizational* category.

A crucial gap in execution existed in our company between the group that created the policies at the enterprise level, and the group that acted in the capacity of our CIRT. On one hand, the policy-makers dealt with almost none of the tactical activities. On the other hand, the CIRT, was dedicated, in large part, to the tactical activities of responding to individual employee security events. The CIRT acted mostly reactively. It wasn't clear who would be required to **proactively** satisfy the confidentiality, integrity and availability requirements

[2] "Organizational Structures for Information Security" Roberta Witty, June, 2003. Page 4

raised by the enterprise policies. Nearly all of them fell into the tactical category. It wasn't clear how they would be satisfied, either. The gap, as it turned out, needed to be filled by the business units.

Our BU security team began to put effort toward activities in the tactical category, but they were largely uncoordinated with activities in the organizational category. We acted, figuratively, as the Dutchman with his finger in the dike[3] preventing the spread of viruses, but with many questions about the structure and intent of the dike.

What made the team operation so difficult, is that most of the effort was put into work in the tactical category without ensuring that the work on organizational category items was consistent with the effort expended at a division and corporate level. The tactical issues must always be evaluated in light of the organizational issues because the organizational issues have an over-arching influence on and are intertwined with the tactical ones. Solutions to issues in either category should not be developed in a vacuum.

An agenda of five items made up the initial effort for our business unit's security team. They were: Virus and Threat Response, Asset Tracking, Network Intrusion Detection, Host Intrusion Detection, and Network Segmentation. This list consists of items that fall into both categories. The items that I consider to be tactical are: Virus and Threat Response, and Asset Tracking. The items that I consider to be organizational are: Network Intrusion Detection, Host Intrusion Detection, and Network Segmentation.

In the next sections I will describe the challenges, pitfalls and successes of items in both categories. My assumption is that the reader is looking for best practices that can be used to implement a security team in their own business unit. Therefore, my goal is to steer the reader toward best known methods (BKMs) that will satisfy the reader's search.

Tactical Category

When the team formed, circa February/March, 2002, the immediate need was to ensure that servers were being patched to mitigate the extant vulnerabilities. For servers running Microsoft Windows™, the current threat was announced by bulletin MS02-005[4]. Our team sparingly addressed vulnerabilities on other platform(s), and in a way that was much less organized than our response to Windows™ threats. The viruses, worms and threats that we were responding to near the time our team formed were SNMP[5] and Life Stages.

Our response methodology to these vulnerabilities was to identify the total available market (TAM) of vulnerable servers, and then begin the process to

[3] See online Webster's at http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=dike
[4] Microsoft Security Bulletin MS02-005.
[5] SNMP = Simple Network Management Protocol.

mitigate the vulnerability, usually by applying a vendor patch. As the patch was applied, a total count of patched servers was kept. The percentage complete was the number of servers patched divided by the TAM. Much attention was paid to keep up-to-date values for the completion percentage and report that result. Unfortunately, the methodology relied on mostly manual procedures, typically compiling results into spreadsheets. An example of one of these spreadsheets is found below:

Reporting Group	Percent Complete	Total Available Market (TAM)	Total Mitigated
BU Group A	58%	125	73
BU Group B	36%	494	178
BU Group C	96%	53	51
BU Total	45%	672	302

What this method lacks is specificity. One is unable to identify a specific server that is in need of a patch using this aggregated data. An improvement to this process would be to capture the IP address or hostname for each server in the TAM, and be able to determine if the patch was applied. There are tools that can aid in this approach. For example, Microsoft's Baseline Security Analyzer[6], eEye's Retina[7] vulnerability scanner, or Shavlik's HFNetChk Pro[8] tool.

These efforts were framed by a service level agreement (SLA) that defined the maximum length of time allowed for a patch to be installed. The initial one was created by the policy-making security group, and the date varied by the severity rating of the threat. Logically, a threat with a high rating was allowed the least amount of time to deploy. The SLA was defined by corporate policy-makers, but without the partnership of the BU security teams. There are operational constraints that must be accounted for when creating the agreement, and the BU teams are the best ones to consult in these areas. Because the first version of the SLA lacked this partnership, the agreement was contentious, ill-informed and lead to begrudging compliance and missed deadlines.

The second agenda item in the tactical category that we undertook was asset tracking. A system that is vulnerable to attack must be identifiable in order to mitigate a threat. A company the size of mine has thousands of servers, and the challenge to manage these assets is formidable. The rate with which these server assets move and change requires a robust system to track them. The tools mentioned above are all based on the fact that a server has a unique identity when it is part of a computer network. It's that fact, also, that is behind much of the hacking activity on the internet. For example, IP address spoofing is a common way to attempt unauthorized access to a system.

[6] A free download is available from Microsoft's website, www.microsoft.com.
[7] A 15-day evaluation version can be downloaded from eEye's website, www.eeye.com.
[8] A free version, HFNetChkLT, is available at Shavlik's website, www.shavlik.com.

The asset tracking tool should accurately and efficiently link together two types of information about the asset: contact information for the system administrator (SA) and the SA's manager, and the identifying information for the server. The contact information should include phone and pager numbers, email addresses and desk or office location. The server identifying information should include hostname, IP address, fully qualified domain name (FQDN), and geographical information such as the region, country, site or campus, building, room and floor location where the asset is physically positioned. When a threat against these assets occurs this information can be used to notify the individuals that can mitigate the vulnerability using down-the-wire technology, or to direct on-site personnel to the location of the server should something drastic like a hard power-down or removal from the network be required.

Unfortunately, success in completing this item was (and is) elusive. There are many factors that have caused delays in reaching an end state system that accurately and comprehensively tracks our computing assets. However, we have continued to emphasize that **a central data store must be used for asset tracking**. Having a single system of record is critical to an integrated tracking system. A solid effort should be funded and made to model the data to be stored in the asset tracking system. Without a validated, comprehensive data model, inconsistencies will derail operations, confidence in the tool will be eroded, and constant, negative implementation issues will arise.

When tackling the tactical category of security activities, it is important to make good decisions about the tools that you will use. Choose your tools carefully. When tools proliferate without good integration, it can become a barrier rather than a boon to productivity. The suite of tools should be capable of vulnerability assessment, reporting on the current configuration of your computing infrastructure, and able to perform remediation tasks using down-the-wire ("hands-off") techniques that require minimal administrator intervention. Where possible, integrate all the tools that you use. Finally, your processes should support your tools, and vice versa.

Organizational Category

The activities in the organizational category consisted of three areas: network and host Intrusion Detection Systems (IDS), and Network Segmentation. I have categorized them this way because they involve strategic planning that typically requires approval of management. The solutions developed to address these areas also involve some policy development, an understanding of the existing IT risk management (both program and policy), and business security architecture which are all tasks that require the involvement of managers who have the authority to make centralized decisions for the enterprise. Since these conditions did not exist in our business unit, these agenda items were never completely addressed.

Our BU participated in initiatives that were underway for these activities to the extent it was possible. However, the development of enterprise-wide programs to manage these areas advanced in parallel to the work our BU security team did on tactical activities. For example, an intrusion detection program was begun, and our business unit became an early pilot group for the deployment of a host-based IDS (HIDS). We controlled the HIDS policies and parameters for our BU, but the strategic, corporate policies were developed and the key decisions were made at a much higher level. Along a similar vein, the program to segment the computing network, was conceived by our corporate security architects but its vision and goals for our BU were not well defined. It wasn't until our BU (and the business unit we support) was negatively impacted by the SQL Slammer[9] virus, that we became an active participant in the definition and deployment of a network segmentation[10] strategy.

Our security team focused primarily on the tactical category activities and devoted minimal effort on the organizational category activities, though not by choice. Time and resource constraints made that a reality. If you use the number of virus infections as a standard of measure, we were largely successful at securing our computing assets. Our company employs a continuous process improvement methodology to conduct our business. Because of this, throughout the stage of establishing our BU's security team, we focused on the ways in which we could improve our strength in the tactical and organizational category activities. We were committed to achieving success in both. We learned a great deal from the effort, and we carried that into our current operating model which I will discuss in the next section.

The BU Security Team Today

Our security team today is working hard to operate more like a comprehensive program than a short-lived team. This requires a mindset and structure of program management rather than team management. The Programme Management Group PLC (PMG) defines program management as, "the co-ordinated management of a portfolio of projects to achieve a set of business objectives." You will see below that we have several projects in-flight, and our business objective is to drive our security defense in depth strategy into all four areas of the security lifecycle: prevention, detection, response, and prediction.

The projects we are working on reflect our desire to integrate our tactical and organizational category activities into an integrated program with a single focal point. We continue to place a heavy emphasis on prevention. We continue to expend a lot of effort on server patching activities because this brings the highest return on the time invested. One project that is aimed at increasing the return on investment is security tools development.

[9] SQL Slammer appeared on January 24, 2003.
[10] Network segmentation is the physical division of a network into separate parts or segments.

As I stated earlier, we tracked the percentage of compliant servers (those that were patched) using a manual spreadsheet method. Beyond the operating inefficiencies of this method was the increased likelihood of error, the lack of speed in acquiring the data, and the ability to confirm the results using a mechanized tool. A much preferred method to collect this data is using down-the-wire tools. We are working to bundle the ability to do vulnerability assessment, reporting and remediation within a single tool suite on the Microsoft Windows™ platform. An integrated tool for servers running under Unix needs to be developed separately. The goal we set is to enable the system administrator to determine if a vulnerability exists then to report on the patching condition of the server. Once that information is known, we want to enable him or her to deploy a patch down-the-wire to the vulnerable server using information presented in the report. A key challenge is ensuring that the tool supports and enables the business processes. In other words, the tactical capabilities must support and be consistent with the organizational activities and policies.

A project to develop a patching methodology is underway concurrently with the tools project. The projects go hand-in-hand. The goals are twofold: first, document the business processes of the teams involved with patch deployments; second, identify and evaluate the environmental constraints that impact deployments. When these goals are achieved, each operational unit will be aware of the part they play in the processes, and then how they can manage the constraints to identify an optimal time to deploy a patch. This methodology should extend to any server regardless of the operating system or hardware platform.

Once our BU security team was organized as a true functional team with dedicated human resources, a project to segment the network into secure enclaves began. This task addresses the prevention area of the security lifecycle. Both logical and physical segmentation is being designed. The logical segmentation will segregate different applications into their own subnets. The physical segmentation will place server hardware to designated secure “landing zones” within the data center. This facilitates easier disconnection from the network, should that become necessary, by collocating servers within a reasonable distance of each other. It also improves the physical security of these assets by placing them in a controlled access environment.

We have stronger affiliations now with the enterprise security teams and those that have a focus on security architecture than we ever did in the past. As I stated earlier, the main challenge in establishing our BU security team was the chasm that existed between us (the tactical group) and the enterprise policy-makers (the organizational group) because each one was working in isolation. Therefore, it became imperative for us to create a vacuum-resistant partnership so that each benefits from the influence and knowledge of the other. To this end, we attend regular meetings to stay connected to individuals and teams who

manage and develop the enterprise strategies and policies. These meetings include a management review committee, a technical review group, and a group that manages infrastructure strategy and architecture. The primary reasons to attend these meetings is to represent the interests of our business unit, and have input to strategy and policy development.

An important component of program management is communication. Our security team reports weekly on our progress. These metrics and indicators reports give our stakeholders a view of our performance goals in several areas. Of primary concern is our progress in deploying patches to our infrastructure servers for the known vulnerabilities. Our company rates the vulnerabilities, and those given a High or Moderate rating require deployment by an agreed upon deadline. Our progress toward 100% compliance by the deadline is the most closely scrutinized metric. Another area is the number and percentage of servers that can be monitored for compliance by our centralized configuration management tool. We are striving to have 100% of all our servers able to be monitored down-the-wire. The final area that we report on is the number and percentage of servers that have been registered in our asset management system. This is an indicator for the ease with which a server can be identified and located in the event of an attack. In order to defend a server, you need to know where it is. Our goal is to register 100% of the servers in our environment.

Our security team is in a better position now than ever before to achieve the security goals we have set for our business unit. Our mission to "transform the way we evaluate, deploy and maintain a secure eBiz computing environment" can be accomplished with the lessons we've learned and the progress we've made since we started. It is important to form your own team by understanding the needs of your business unit, devising a plan to fulfill those needs, and then partnering with the corporate security resources to integrate into the overall enterprise security strategy. In so doing, your likelihood of success will be very high.

List of References

Network Security Center, University of Chicago. "NSC: Physical Security." 21 January, 2000. URL: http://security.uchicago.edu/docs/physicalsec.shtml (July 11, 2003)

Electronic References. "Computer Viruses: Infection Vectors, and Feasibility of Complete Protection." 2003. URL: http://www.electronicreferences.com/view.php/Technology/741.HTM (July 11, 2003).

CERT Coordination Center. "What is a Computer Security Incident Response Team (CSIRT)?" May 8, 2003. URL: http://www.cert.org/csirts/csirt_faq.html#1 (July 12, 2003).

Meridian. “N2N Security Practice Information Security Requirements Model.” 2003. URL: http://www.n2nsolutions.com/mitsisecurity/Requirementsmodel.pdf (July 11, 2003)

Security Focus. “Initial analysis of the .ida ‘Code Red’ Worm.” July 17, 2001. URL: http://www.securityfocus.com/archive/88/197488 (July 11, 2003)

Security Focus. “’Nimda’ worm hits net.” July 17, 2001. URL: http://www.securityfocus.com/news/253 (July 11, 2003)

Gartner. “Organizational Structures for Information Security.” Roberta Witty, June, 2003.

Microsoft Corporation. “Microsoft Security Bulletin MS02-005.” February 11, 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-005.asp (July 12, 2003)

CERT Coordination Center. “CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)” February 12, 2002. URL: http://www.cert.org/advisories/CA-2002-03.html (July 12, 2003)

Symantec. “VBS.Stages.A” December 7, 2000. URL: http://service4.symantec.com/SARC/sarc.nsf/html/VBS.Stages.A.html (July 12, 2003)

Microsoft. “Microsoft Baseline Security Analyzer.” 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp (July 13, 2003)

eEye. “Retina Network Security Scanner.” 2003. URL: http://www.eeye.com/html/Products/Retina/index.html (July 13, 2003)

Shavlik. “HFNetChkPro 4.0” 2003. URL: http://www.shavlik.com/ (July 13, 2003)

Netservers. “Segmenting your network.” 2001. URL: http://netwervers.co.uk/segmenting.html (July 16, 2003)

The Programme Management Group PLC. “Programme Management Definitions.” 2003. URL: http://www.e-programme.com/articles/proj_def.htm (July 16, 2003)