GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Sun Tzu and the Art of (Cyber) War: Ancient Advice for Developing an Information Security Program

Matthew K. Miller

Version 1.2b
April 2, 2001

It's been over 2500 years since Sun Tzu, the famous Chinese military philosopher, wrote his timeless work The Art of War. Today, his tenants for conducting military operations are taught and applied in the United States military. If Sun Tzu's principles can be applied to the modern battlefield, can they be applied to the battlefield of cyberspace? Though the battles fought are quite different from ancient China, Sun Tzu's philosophies can aid when setting up a security program at your company.

In The Art of War, Sun Tzu wrote that a country must have sufficient military capability, "Military affairs are a country's vital political concern," and a country must have a comprehensive security strategy, "the lands that are lethal or safe and the ways that cause existence or destruction must never be taken lightly". (Sun Tzu 37) How appropriate this is for the cyber landscape! Any company doing business on the Internet is concerned with defending it's network and critical assets against unauthorized intrusion or attack. Sun Tzu writes about five key areas that apply to a company developing an information security program: Leadership; Soldiers; Rules; Weapons; and War Plans.

First Steps: Leadership

Sun Tzu stated, "Leadership causes people to follow their superiors willingly; therefore, following them in death and in life, the people will not betray them." (Sun Tzu 38) A successful security practice starts with the head of the company empowering a Security Manager and flows down through the security team members. Sun Tzu addressed the ability of the political authorities, "Which Lord has better leadership?" (Sun Tzu 39) A company which internalizes security at its core, lays the foundation for a successful security practice. This internalization starts at the top, "Senior management has to see the inseparable link between computer and network use and computer and network security." (Avolio 3)

The security practice must have strong leadership and credible skills. This position requires an understanding of the company's business as well as best security practices. A balance must be struck between these two areas. Avolio talks about the importance of this balance by saying that security "premises firmly grounded in reality, that take into account the needs for both usability and security, gives us the freedom to thoughtfully and calmly provide the security we need, in a manageable way, while still delivering required services and enabling profitability." (Avolio 3)This position is also the interface between management, which is focused on the business goals of the company, the security team, which is focused on protecting the company, and the systems administrators,

© SANS Institute 2000 - 2005 Author retains full rights.

which are focused on the functionality of the infrastructure. This balance is very tenuous; compromise and understanding are indispensable. Unfortunately, this is generally where the breakdown in many organizations occur; mainly due to lack of understanding. Forums, such as a security steering group, allows representatives from all three areas to meet, discuss issues, and make decisions to maintain the balance between security, functionality, and business requirements. Around this leader, the security team needs to be built.

Building Your Army

With the commander appointed; the army (security team) must be formed. The make up of this team is solely dependent on the company. Size, type of business, dependence on the Internet, and types of resources are all factors that contribute to the make-up of the team. The first step to building this team is to identify the middle managers, or the field commanders.

When developing a security program, it is imperative to have a good middle management. Sun Tzu wrote, "Commandership requires wisdom, credibility, benevolence, courage, and discipline." (Sun Tzu 38) Wisdom comes from the manager listening to the security staff under their command. The staff has the technical knowledge and understanding of the systems. The manager needs to work their recommendations into the security strategy of the company. The manager needs to be credible in the eyes of the staff and the company employees. Experience, certifications, and knowledge quantify this credibility, but the manager's actions provide respect. Benevolence, courage and discipline are also valuable qualities for a security manager when dealing with a variety of unpredictable situation. With these layers of management in place the "chain-of-command" or reporting structure is taking shape. Staff requirements are still necessary to round out the team.

As stated before, staffing is dependent on the needs of the company. Finding the appropriate staff that meets the requirements laid out by management is very important, but difficult. Consultants and managed service providers are ways of augmenting the staff in positions that can not filled, "Depending upon your internal capabilities, using an ASP (application service provider) or SSP (security service provider) may make sense." (Paul 5)

Once the staff is in place, an ongoing training plan will maintain the level of their expertise. When addressing this Sun Tzu asked, "Which side's warriors and soldiers are better trained?" (Sun Tzu 39) Quality of on-going training is an important differentiator in information technology. New hacker attacks and techniques crop up every day. In order to deal with these effectively, the team must be equipped with the knowledge to succeed. Studying materials found on hacker web-sites, attending security seminars (such as SANS Institute Seminar Series), and participating in security forums are ways to keep up with the ever changing hacker community. This information arms the security team with the knowledge it needs to address the next step; setting the company's security

© SANS Institute 2000 - 2005 Author retains full rights.

policy.

© SANS Institute 2000 - 2005, Author retains full rights.

Rules: Creating the Company's Security Strategy

The security team can not operate above the law. Sun Tzu said, "The rules are in regulations for mobilization, official duties, and the management of materiel." (Sun Tzu 38) The greatest security professionals are worthless without a solid security policy for them to enforce. Policies and procedures define what needs protection, why it needs protected, and from whom it needs protection. In the article, "Opening Your E-Business Perimeter," Brooke Paul writes,

> "To implement a defense-in-depth architecture, you need to understand the infrastructure systems and application involved and the risks associated with each. If one layer in your infrastructure has a known vulnerability, you can place controls in another layer to provide protection and alert capabilities." (Paul 2)

By conducting and completing a risk assessment, the team sets the tone for a security program by defining what and how assets are to be secured. How the company employees conduct business is also included within these rules. The question Sun Tzu poses is, "Which side carries out rules and orders more thoroughly?" (Sun Tzu 39) How effective are policies and procedures if the staff and employees do not follow them? Using shortcuts or refusal to follow policies and procedures bypasses your network's security and potentially leads to exposures. For example, a company's policy states that putting a hole in a firewall must go through the change control process and a review by the security team. The procedure states that a risk analysis of this hole be provided along with specific steps to open the hole. This is a sound policy and procedure that prevents potential mistakes that could expose the network to unnecessary risk. One day the firewall administrator receives a walk-up request to allow Internet Relay Chat (IRC) so the individual can participate in an on-line conversation. The individual has the correct credentials to open this service, but is very busy. Rather than fill out all the paperwork, they just open the port to allow all traffic through the firewall. Unfortunately, in the administrator's haste, they allow all IRC to traverse the firewall and has opened a major hole in the network's security. While conducting the network survey, examine the company's policies and procedures, as well as, the execution of them. In addition to policies delineating <u>what</u> can and can not be done, security policies should address roles and responsibilities.

Separation of Duties is a key concept that should be adopted into all security practices. Separation of duties is the, "dividing of roles and responsibilities so that a single individual cannot subvert a critical process." (Vallabhaneni 142) Ensuring that no one position has absolute power over the operating environment minimizes the risk of a total compromise from within the organization.

Security policies also apply to the user community. Appropriate use policies governing email, Internet usage, and personal computers provide a framework

© SANS Institute 2000 - 2005 Author retains full rights.

for how the users can conduct business. These policies should be concise and understandable. User's attention will begin to wane after a few pages. These individuals are the weakest link in your security program, due to their lack of knowledge.

Setting the rules is only half the picture. Rules are useless without enforcement. Sun Tzu realized this to be a critical issue, "Which side has clearer rewards and punishments?" (Sun Tzu 39) Frederick Avolio also addresses this concern,

> "Security policies alone have no teeth. Corporate management support supplies that. If senior management does not support parts of the work, they are essentially dead." (Avolio 3)

There is a balance, however. You do not want to inspire a climate of fear. The operating environment's primary purpose is to enable employees to conduct business more efficiently. Striking the balance between efficiency and security is the key.

These policies should also detail what is to be protected. Identifying critical computer assets, classifying risks and threats is the step prior to establishing your network security defenses.

Weapons: Establishing Defenses

Your security program now has it's management in place. The security staff is hired and formal training plans are in place. The company's security policy is formalized and critical assets have been identified. The next area to address is the protection of the critical assets within your infrastructure. In war, whether conventional or cyber, victory is determined by the army with the best weapons and people. Sun Tzu asked a simple question when evaluating competing armies as to who the victor will be, "Which side has stronger weapons and people?" (Sun Tzu 39) As we addressed earlier, having strong leadership and trained staff is essential. The second part of the equation are the weapons that the army uses.

Your first line of defense against external intruders is your perimeter defense which includes firewalls, access control lists, and physical access control. The purpose of perimeter defense is to, "build a virtual wall around the network, controlling and securing all access into and out of it." ("Thinking" 2) How does a firewall contribute to this goal? According to the article, "Thinking About Firewalls",

> "the purpose of the firewall is to prevent unauthorized users from accessing computing resources on a private network, and sometimes to prevent unnoticed and unauthorized export of proprietary information." ("Thinking" 1)

© SANS Institute 2000 - 2005 Author retains full rights.

Access Control Lists (ACLs), much like firewalls, govern accessibility to information or assets. ACLs can be placed on specific interfaces on a network segment, virtual private network tunnels, or other types of secure connections. The best technical perimeter countermeasures can be circumvented if an intruder gains physical access. Access badges that restrict entry to network and server operations, security guards, and locked computer cabinets are common physical access control measures. According to an article by Allen, no perimeter security is infallible, so additional layers of security are needed, "Intrusion Detection is needed because firewalls cannot provide complete protection against intrusion. Experience teaches us never to rely on a single defense line or technique." (Allen 15)

Sun Tzu realized, as savvy security managers do today, that security does not eliminate risk; rather it reduces the risk to a point that is acceptable to the type of information they are protecting. An interior alarm system functions as a safety net for when perimeter security fails. Intrusion detection systems (IDS) are the cyberspace equivalent of physical security alarm systems. According to the white paper "State of the Practice of Intrusion Detection Technologies", "the goal of intrusion detection is to positively identify all true attacks and negatively identify all non-attacks." (Allen 7)

IDS comes in two forms: network and host based. Network based IDS scans network traffic searching for abnormal activity or known attack signatures. If an intruder is able to circumvent your perimeter security, the network IDS will be looking for them. Host based IDS resides on critical assets. These sensors watch for tell-tale signs of operating system and file integrity compromise. Some of the tell-tale signs that host based IDS look for are: account alterations, failed logins, and file system tampering. File integrity checks if critical files have been altered. This is usually done on files that contain information that rarely changes, but must be accurate. Web pages and price lists are some files that are commonly monitored this way. Alarm systems are quite effective in notifying the appropriate people when an attack is occurring, if the system is being monitored. The company must address manning of these systems 24 hours a day. Managed Service Providers are a good alternative for in-house monitoring. There are some types of attacks that IDS can not detect; mainly these are considered "asynchronous" attacks.

Asynchronous attacks are not under the direct control of an intruder. These are no less damaging than directed attacks. A very common asynchronous attack is the use of email borne viruses. Viruses are computer programs that execute without the knowledge of the user of the system. Email is a wonderful delivery system for the spreading of viruses, since most firewalls do not scan email traffic for attacks. The hidden code of viruses, very often, contain malicious commands that can compromise or destroy the victimized computer. Anti-virus software combats these viruses in multiple tiers of defense. Anti Virus

© SANS Institute 2000 - 2005 Author retains full rights.

appliances can reside on email servers, client servers, and even network based appliances to search for virus signatures and prevent infestation. Host based IDS can also combat viruses, when they activate the malicious code. If the virus attempts to tamper with the operating system, the host based IDS will detect the attack. All these tools to defend your network are very effective when used together, as long as they are maintained.

Sun Tzu wrote that regular maintenance of these weapons is of utmost importance. This is very true with information security tools as well. Since these tools are written by humans, they are susceptible to mistakes which are called bugs. Bugs can lead to vulnerabilities that an attacker can exploit to gain access. Manufacturers are constantly fixing these bugs with updated code called patches. System administrators must maintain the most up to date patches to reduce the chances of being exploited. New attacks and viruses are cropping up every day, as the October 2000 article "Improving the Security of Networked Systems" addressed:

> "...evolving attack methods and software vulnerabilities continually introduce new threats to an organization's installed technology and systems. Thus, even vigilant, security-conscious organizations discover that security starts to degrade almost immediately after fixes, workarounds, and newly installed technology are put in place." (Allen)

Anti-virus and IDS signatures need to be updated very frequently to counter these new threats. The focus of our weapons thus far has been against external intruders; however internal users need to be monitored as well.

All users must login to the network before they are able to access company information stored on central servers. The login process includes authentication, that is validating the identification of the user and determine what activities they are permitted to conduct. Username and passwords are the most common method of authentication. The username identifies the individual while the password, a secret word or string of characters, validates that identity. The problem with this authentication mechanism is the assumption that the secret password remains secret. The individual could tell someone the password or it could be easy for an intruder to guess. Knowing both the username and password of another individual and using those credentials for your own activities is known as identity theft. To reduce the risk of this occurring, stronger authentication mechanisms should be employed. The common theme with authentication mechanisms is that the user has something and knows something. This mechanism is used with an ATM machine; you have an ATM card and know the PIN number. The combination of the two identifies and validates your identification and lets you withdrawal money from your account. With one-time passwords, the use of a token is the "something you have". It is

© SANS Institute 2000 - 2005 Author retains full rights.

usually a credit card sized device that displays a number. This number will change periodically. When authenticating, the use of the number with the "something you know", a password, provides a stronger form of authentication. The process of logging in should be monitored for failed attempts, logins during non-work hours, or other suspicious activity.

The key to all these tools is to fit within the security framework you have established thus far. Technology should not be implemented without integrating it properly with your existing infrastructure. Not all tools are appropriate for all operating environments. Now that the defenses are in place, you need to look at the worst case scenario: all your defenses are defeated.

War Plans: Preparing for the Worst

The best laid defenses will eventually fail. When that happens, the security team needs to turn to preexisting battle plans. Two of the most important plans are a disaster recovery plan and an incident response plan. Disaster recovery addresses what happens after a natural or man-made disaster. The scope of this plan greatly depends on type of business and information the company has identified as critical. Remember those critical assets? This plan should address each of those assets and how their services can be restored. Sun Tzu realized the need for flexibility when it came to these factors, "Which side takes better advantage of the cyclic natural occurrences and the geographical factors?" (Sun Tzu 39) The disaster plan needs to be general enough to address any type of disaster, yet specific enough to give direction in a time of crisis. "To avert potential contingencies and disasters or minimize the damage they cause organizations can take steps early to control the event." (Vallabhaneni 337). The plan should follow three basic steps: preliminary emergency response, recovery actions, and resumption of service for critical systems. (340) This plan needs to be practiced and continually updated. As your networking environment changes, the disaster recovery plan evolves as well.

Like the disaster recovery plan, the incident response plan needs to be in place before it is needed. The critical steps that should be included in the incident response plan are: regain control of the situation, analyze the intrusion, recover from the incident, improve your security to prevent the same type of attack, reconnect to the Internet, and update the security policy to reflect changes. ("Steps" 1) Entire books discuss the creation of these types of plans; it is critical that both Disaster Recovery and Incident Response are addressed in depth. If your company waits until an incident or disaster occurs, it will be too late and all the work accomplished in the previous steps will be for nothing.

© SANS Institute 2000 - 2005 Author retains full rights.

Tying it all together
Sun Tzu's final comments on this subject were,

> "All generals have to learn these five in their entirety. Those who know them will be victorious. Those who do not know them will not be victorious. Then, they are verified through surveys to assess their status." (Sun Tzu 38)

All five of the areas are critical, but it is not a one-time effort. Security is a process, not a product. When you complete the five steps, reassess them on a recurrent basis. Networks are not static entities, they continually evolve with your business. Periodic vulnerability and risk assessments should be a fundamental part of your security program.

After comparing Sun Tzu's teachings with fundamental competencies in information security, it is clear that warfare strategies are quite applicable. A wise historian once stated that he who does not learn from history, is doomed to repeat the mistakes of the past. When creating a new security program or reevaluating your existing program, look at the five areas of Sun Tzu's teachings: Leadership, Soldiers, Rules, Weapons, and War Plans.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

References

Allen, Julia, Christopher Alberts, Sandi Behrens, et. al. "Improving the Security of Networked Systems." Cross Talk. URL: http://www.stsc.hill.af.mil/crosstalk/2000/oct/allen.asp (March 5, 2001)

Allen, Julia, Alan Christie, William Fithen, et. al. "State of the Practice of Intrusion Detection Technologies." Networked Systems Survivability Program. URL: http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf (March 25, 2001)

Avolio, Frederick M. "Best Practices in Network Security." Network Computing. March 20, 2000. URL: http://www.networkcomputing.com/1105/1105f2.html (March 25, 2001)

Edwards, Mark Joseph. "What's Your Policy?" In Focus. August 16, 2000. URL: http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=9764 (March 5, 2001).

Huang, J.H. Sun Tzu: The New Translation of The Art of War. New York: William Morrow and Company, Inc., 1993.

Paul, Brooke. "Opening Your E-Business Perimeter". Network Computing.com. January 8, 2001. URL: http://www.networkcomputing.com/shared/printArticle?article=nc/1201/1201f1afull.html&pub=nwc (March 16, 2001).

"Steps for Recovering from a UNIX or NT System Compromise." CERT Coordination Center. URL: http://www.cert.org/tech_tips/win-UNIX-system_compromise.html (March 25, 2001)

"Thinking About Firewalls V2.0: Beyond Perimeter Security" 1993, updated 1996. URL: http://pubweb.nfr.net/~mjr/pubs/think/ (March 16, 2001).

Vallabhaneni, S. Rao. CISSP Examination Textbooks, Volume 1: Theory. Schaummburg, IL: SRV Professional Publications. 1st Edition.

© SANS Institute 2000 - 2005 Author retains full rights.