Global Information Assurance Certification Paper

A Security Model for Higher Education:
The Information Protection & Security Loop

GSEC Assignment version 1.0
Lance D. Jordan
August 15, 2002

Introduction

Higher Education is a dynamic learning and working environment for students, staff and faculty. The truly successful schools are able to adapt to changing customer needs and provide the "value-added" that differentiates them from the competition. Providing secure and reliable information technology resources to further the goals of the institution are critical tasks to the success of the educational experience. The successful accomplishment of these tasks is no small feat for professional IT staffs that are under-resourced.

What is it about the computing environment within public higher education institution that makes it unique from other environments? According to the recently released report prepared by the Educause/Internet2 Computer and Network Security Task Force in July 2002, "It (higher education) is a complex, technologically robust community that requires and achieves broad access to information and flexible, high-speed communications. The open, innovative values of higher education are, in the end, those of the nation. Their computers and networks represent, in many cases, the emerging systems of the future. Successful security implementations in higher education can serve as guideposts for the nation at large." [1]

Two common values held by most communities of higher learning are academic and intellectual freedom. This significant need to collaborate with colleagues, both internally and externally, places important challenges on the IT infrastructure. Tremendous efforts are made within higher education to be inclusive rather than exclusive in the types of services provided by central computing and in the methods used to deliver these services to its customers. Most of the academic community consider access and openness a right rather than a privilege and are severely opposed to any unjustified restriction of their use of networks and computers. As cited in the Educause report, "a recent study by the National Research Council stated that some of the payoffs from this type of environment support the conclusion that the open nature of the Internet and campus networks has been an important factor in the rapid and flexible development of innovative applications." [2] Now more than ever, those responsible for securing the computing infrastructure (the supporting) and the users (the supported) of the computing environment have to function as a cohesive team with the agility and foresight of skilled combat fighter pilots. Even though I am not talking about "life or death" situations, the ability of the organization to achieve its goals is highly dependent upon the responsiveness and reliability of the staff within the IT services department.

The purpose of this paper is to explain how I adapted a process model developed by Colonel John Boyd, USAF, called the OODA (Observe, Orient, Decide, and Act) Loop to my higher education environment. I think everyone will agree that today, information and computing assets are mission critical resources and whether you are responsible for computer security within a higher education institution or the corporate world there are many similarities in the decision-making process used by both fighter pilots and security specialists.

Situation

An external consulting firm has just evaluated your university's information protection and security posture and concluded that the university needs to establish an organization responsible for developing a university-wide security program. Congratulations!! You have just been selected to lead the computer security program at your favorite institution. It can be both a blessing and a curse to be the first on your block to start a security program for a large organization, especially a large public institution of higher education. Although there is no shortage of security information available in the public domain; defining a process that can be used to pull it all together, digest it, and help in the selection of a course of action, and then repeat the process would be helpful. What to do?

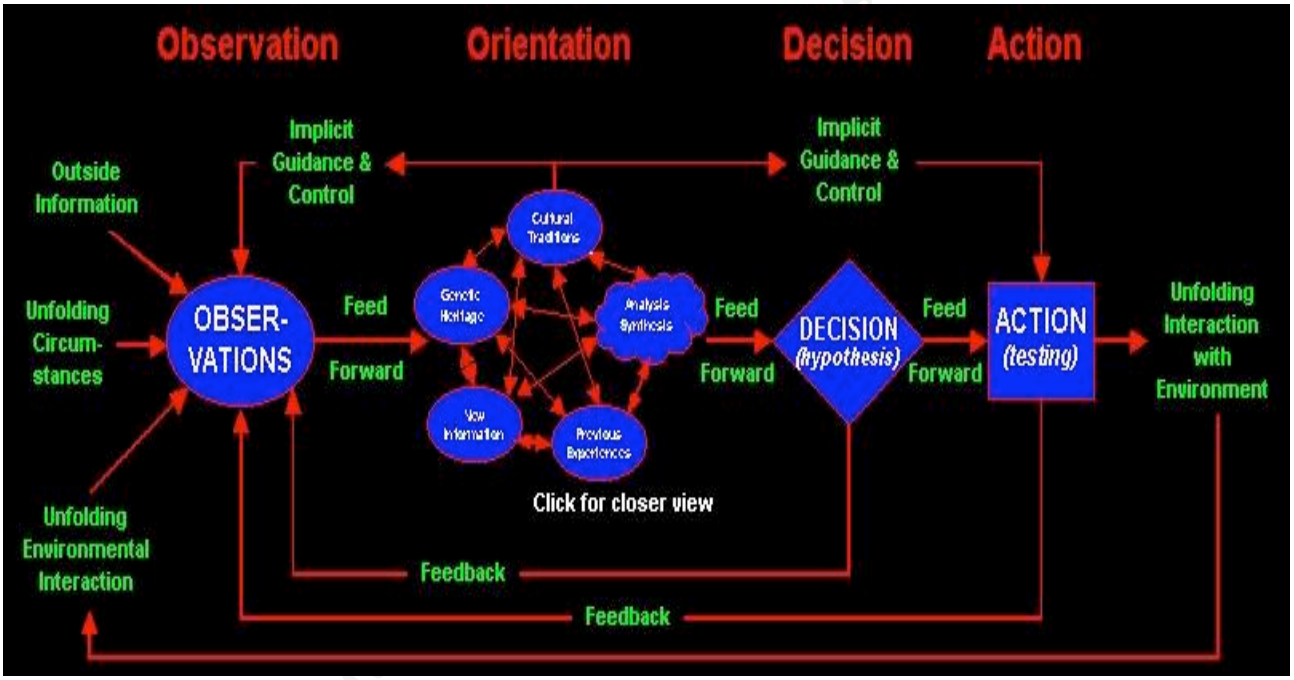
Two years ago I was introduced to this very situation. I started looking for a process model that would be applicable and understandable to both staff and management. One thought was to adopt a marketing analysis model called SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats) but then I remembered Colonel Boyd's OODA Loop model. I was first introduced to the term OODA Loop while attending the Marine Corps Command and Staff College in the late 1980s. The Marine Corps was in the process of revamping their war-fighting doctrine and there were numerous discussions and case studies on how to get inside your opponent's "decision cycle." [3] Why not apply it in the computer security area? Fortunately I was able to take advantage of this model developed by Colonel John Boyd, USAF and adapt it to my own environment.

To often we look to apply a technology solution to a problem that is grounded in highly unpredictable human behavior. Anyone with a computer with access to the Internet is the first line of defense and the most likely point of entry for a constantly aggressive and increasing dangerous foe, the determined hacker or the curious script kiddie. One of our toughest challenges is to convince our users to recognize that they have a role to play in protecting their personal information and in applying the OODA Loop every day they will develop good computer security practices. If you have a large organization similar to mine with over 25,000 hosts, various operating systems and users with a wide range of skill sets, you have to recruit them into you larger security strategy.

Colonel John Boyd, USAF and his OODA Loop

In his article about agile corporations Adrian Ferrell writes, "The late Colonel John Boyd was a US Air Force fighter pilot of exceptional ability. After his initial combat experience in the Korean War he devoted a great deal of his life to studying strategy and

warfare tactics. The OODA Loop was the result of an investigation led by Boyd into the reasons why the U.S. Air Force in Korea had such a high kill ratio, 10:1, with aircraft that were far inferior to the enemy's jet fighters. Over the years his work has seen application within corporate America. He wore the Air Force uniform for 24 years." [4] Colonel Boyd was a legend in his own time, partly because of his reputation of being out there on the edge, but mostly because he challenged the system. While on active duty and into retirement he made more contributions to fighter tactics, aircraft design, and the theory of air combat than any man in Air Force history. Perhaps most importantly, Boyd was instrumental in explaining and disseminating the concept of "cycle time" and "getting inside the adversary's decision cycle."[5]



Diagram[6]

The following is a brief explanation of the model: The first step of this model is to gain knowledge of the strategic environment. Gaining knowledge is an active, not a passive activity. Once you discover valuable sources of information, whether internally or externally, in some cases you can automatically program this information to be fed to your desktop or to others in your team. Secondly, one must be able to interact with the environment and those within it appropriately. This can take the form of personal face-to-face interaction among team members brainstorming issues or queries sent to listservs. You must be able to observe and orient yourself in such a way that you can maneuver into a more favorable position vis-à-vis the opposition. Doing so requires a complex set of relationships that involve both isolation and interaction. Although not part of this paper, I would suggest at this point that a strategy of a "defense in depth" (another term taken from the military) is critical to an overall security strategy because it helps to buy time in order to maintain your freedom of action. In OODA Loop fashion, one must

continually observe, orient, decide and act in order to achieve and maintain freedom of action and maximize the chances for survival and prosperity. Rapidity of action or reaction is required to maintain or regain the initiative. [7] We will now review each step in the model in greater detail.

Observe

As mentioned above take an inventory of what is happening within your own environment and those external factors that have a direct impact on your ability to operate. The purpose of this step is to gather as much information or intelligence on those activities happening around you. The computing environment within most large institutions is open and highly distributed. Within my organization, we have over 25,000 hosts running a variety of operating systems including Windows, Unix, Linux, and MacOS. Our staff and faculty need to collaborate with other faculty and researchers around the country and with state and federal agencies. This creates a constant challenge to maintain an equitable balance between access to information and protecting systems, data and user privacy. I think the key operational term is "Know your business." Every organization, large or small, needs to have a security policy for two very important reasons. One, your users need to know what the boundaries are for acceptable use of the computer systems and two, the computing staff need to know what rules to enforce. According to Gary Bahadur for Login Magazine, "A good policy will be a dynamic living document and provide a good framework for the details that follow in standards, procedures, and guidelines." [8] Take a look at the applicable policies regarding access to your networks and whether there is a policy regarding acceptable computer use. Also, review the appropriate Federal and state laws and regulations. If you find that your organization is lacking in these areas I recommend reviewing some of the reference materials from http://www.cert.org/, http://www.sans.org/, or http://www.nist.gov/. Ensure that your policy is understandable and enforceable. A recommended standard from a federal agency may not be acceptable to the user community within your organization or not enforceable due to the lack of resources or funding.

If you have a computer incident response team (CIRT), take a look at their statistics and look for trends. Gather statistics from your Help Desk staff and the network operations group and look for trends, as well. If you don't have a CIRT, consider establishing one. Http://www.sans.org provides an excellent action plan for dealing with intrusions, cyber-theft, and other security related events. Even in a small highly centralized computing services departments you will find little pockets of critical information that are horded, but essential to helping to complete the picture of the historical and recent experience of the organization. There are many other sources of data that can help complete this picture and just a few are mentioned below:

- Firewall logs (Do you have a mechanism for units to report attempted intrusions similar to http://www.dshield.org/.
- Intrusion Detection System logs (Do you have network or host-based IDS installed and are you getting reports from them?)

- Internal scanning (Are you scanning your internal subnets looking for vulnerable hosts? There are free tools available such as SARA from http://www.sans.org/ for scanning for the SANS/FBI top twenty and Nessus from http://www.nessus.org/.
- Top talkers (Our network operations group uses an accounting model to monitor total upload and download during a set period of time. Any system outside the normal central systems that appears to be serving large amounts of content usually indicates abuse of policy or a compromised system.)
- Self-reporting (Do you have an anonymous self-reporting mechanism for units to report compromises on their systems? Some organizations may be too embarrassed to admit in a public forum that their host's have been hacked.)

Up to this point in this paper the focus has been mainly internal. As you see from the OODA Loop model, external factors play a role as well. Do research on similar organizations and talk to colleagues about their experiences. Attend higher education conferences like those sponsored by http://www.educause.edu/ and computer security conferences like those hosted by http://www.gocsi.org and http://www.sans.org/. You should subscribe to several of the computer security email lists such as Bugtraq at http://www.securityfocus.com/and CERT advisories at http://www.cert.org/.

The transition from the observation phase to the orientation phase will be significantly impacted by the large amount of information gathered and the challenge of filtering the material from the immaterial information. This transition is dynamic and not static, because of the continuous feed of new information into the process. There may be noteworthy data that if overlooked or discounted could result in a miscalculation of the enemy's intent.

Orient

An organizational structure to help synthesize the tremendous data flow that is not mentioned by the OODA Loop model is called a synchronization center. For many years the U.S. Army doctrine referred to this organization as a "fusion cell." This organization is necessary as a central focus point for receiving and filtering the flow of information, especially if the data is coming in from distributed systems or processes. This could be a mission assigned to your computer incident response team, assuming that this group will interface daily to review the status of network and systems. This synchronization center can be a central repository or database or a small cell of people who refine the view based upon the inputs received. The accuracy or reliability of information is determined during the orientation part of the cycle by what information is filtered and how it is organized. You have to pose the question, "What do I act on and what do I ignore?" Even the most highly skilled security staff using the best technology available will be operating in an environment of uncertainty. This is where a sound knowledge base helps to tailor the view of the situation and discount biased views of what is happening around you. The orientation phase is the most critical step in the process, because it sets the stage for our follow-on actions. [9]

Now that you have gathered and analyzed as much information as you and your team can absorb you can start predicting potential behaviors of your enemy. I think that this might be a good time to ask the question, "Who is the enemy?" I think the answer can be boiled down to anyone who can interfere with the normal operations of your computing environment. You will notice that I did not mention the word intent. If someone is having a negative impact on your operations, whether by accident or design, their intent is moot. The level of effort required to clean up a compromise will be the same.

Two other important considerations during this phase of the process are the values and traditions of your organization. Some courses of action may not be permissible or supportable within your environment. Rich Mogul from Gartner, Inc. wrote in his article "Prioritizing Security Efforts: Creating Structure from Disorder," that understanding how security is perceived and how the organization responds to security at all levels is essential. [10] Remember that data can be misinterpreted based on an individual's personal bias. For example, this bias could be based on level of experience; what has been seen or done before or based upon the amount of time available to accomplish task.

Decide

To this point in the process you have surveyed the landscape for both internal and external threats and have synthesized the data into what is really important. Now it is time to make a decision. This is where you decide to take an action that will put you in a better position vis-à-vis the enemy or you need to counteract an enemy's defensive action while on the offensive. This decision could be as simple as creating a new policy or a modification to a current policy or modifying firewall or IDS settings.

For example, two years ago my institution experienced a paradigm shift in the way we used the Internet. We were serving more data to the Internet than we were consuming! The culprit was .mp3 file sharing and it was having a negative impact on our Internet response times. Our bandwidth was consumed to capacity. Needless to say the telephones at the network operations group were ringing off the hook and this issue was elevated quickly to the highest levels of the university. The dilemma, we are staunch supporters of free speech and Internet access and consciously do not manage content unless it violates the law. In other words, we have a privacy policy that prohibits us from monitoring content unless there is an abuse situation. We do not view content (packets) as it transits our network. Managing this challenge without violating our own policy and causing a severe ripple within our own community was a concern. One option that was considered was to purchase more bandwidth.

However, we were faced with a situation of supply not meeting peak demand and throwing more money at the problem would not solve it. In the end we pursued two approaches to the problem. We agreed to an economic model that established a daily and weekly upper limit to bandwidth usage, which was enforceable by our acceptable use policy, and we purchased some additional capacity in bandwidth to give us some breathing room. Our user population was notified in advance of the policy change and the policy was slowly put into practice as top offenders were given warnings as a

teaching and learning opportunity before any adverse action was taken. The behavior modification accounting model has worked. Response times returned to normal and the use of network resources came back down to an equitable level.

Act

The final step in this iterative process, yes it is ongoing and continuous, is action. More than likely one action will be followed by a series of subsequent actions until the enemy cannot react with the appropriate counter measures and he is defeated. According to "Information Operations" by Osborne, "The importance of the process is not the cycle, but the ability to rapidly cycle through the process at a faster rate than your opponent." [11]

For example, when a hacker launches a script kiddie, it is unlikely that the hacker is watching the results of his program in real-time. Just like launching a "scud" missile, the hacker has a general idea of where the target was (range and direction) during the initial reconnaissance or from information gathered from other hackers, but cannot adjust to recent changes in location (changes in IP address or protective measures). For example, when an aircraft drops a dumb iron bomb on a target, a photographic reconnaissance mission has to be flown over the site to determine the battle damage assessment to determine the success or failure of the mission. In a similar fashion, the hacker will have to review log data to see the results of his attack. On the other hand, with the proper monitoring tools on your hosts and networks you can watch the activity, warn users, and counter the effects. Some of these tools could be:

- Intrusion detection systems
- Firewall logs
- Auditing system access logs
- Web server logs
- Email virus filtering logs

Some might say that a lot of what security professionals do is not real-time and that we are in the same situation at the hacker because we have to review access logs and other system logs as well. One of the activities that perform the same function as "preventative medicine," like getting a flu shot is internal scanning.

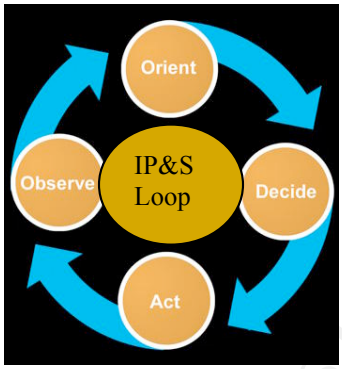
Last summer during the outbreak of Code Red and Nimda, we put together a team to internally scan the university address space using a free scanning program developed by http://www.eeye.com/. Based on the results of the scan, we contacted department computing specialists to inform them of the vulnerabilities and provided advice and support to resolve problems. This was a very intense and time consuming process, but it paid dividends in a reduced number of compromised machines. Pre-planning in advance decreases cycle time and that is the kind of position we want to be in. Some of the things we can do in advance are following the best practices recommended by the GAO:

- Assess risks and determine needs

- Establish a central management focal point
- Implement appropriate policies and related controls
- Promote awareness
- Monitor and evaluate policy and control effectiveness[12]

Within my own organization we established computer use policies and policy recommendations for departmental system administrators. We created an incident response team along with email listservs to exchange information regarding network probes, CERT advisories, our abuse reporting system and other topics security related. We actively scan our own internal networks and provide vulnerability reports to the people responsible for correcting the problems. The university purchased a site license for anti-virus software and we have virus-scanning software installed on our central email servers. However the most important activity is our user awareness program. We know if we can raise the level of awareness of all users, we can avoid many of the issues we see today. We attack this on several fronts by participating in orientation programs for new students, with literature, with ads in the student newspaper, our website and with training sessions for support staff. Our ratio of professional staff to user is about 1 to 200. We know that if we can get our users to use the OODA Loop in their security processes, we will have greater success in protecting our assets.

Conclusion: The Information Protection & Security Loop



Diagram[14]

There was a time when all business decisions were made by senior management the workers were expected to execute without discussion. That model does not work in the information age, especially within the higher education environment. Senior management should set the strategic vision and let lower level management make the operational decisions. As Adrian Farrell at Woodlawn Marketing Services wrote in his article able Agile Corporation, "A major challenge is coping with information and making decisions in such a dynamic environment.[13]

The IP&S Loop can set the framework for the process. The challenge of securing an open and highly distributed system of hosts and networks is partially answered with technology, but according to Scott Culp in "The Ten Immutable Laws of Security Administration," the most important tool is "procedures." He goes on to state, "security is the result of both technology and policy." [15] I would add that the proper application of both in the right amounts is essential, as well.

There are a series of tools that can be applied in this process from acceptable use policies to incident response teams to active scanning and user awareness training. I am a firm believer that most important organizational issues are leadership issues and leaders need to focus their energies on security within the same vein as they focus on the bottom line.

Security is a force multiplier, an enabler, not an expense or cost center. Good security can protect critical information assets, mitigate liability, and enhance the organization's reputation. Knowing that your organization implements sound security practices improves employee productivity and keeps your customers coming back. The higher education is a highly competitive and dynamic environment. Many of the federal agencies who provide grant funding for research are placing stricter requirements on how these funds are used to purchase computer equipment. In addition they are dictating baseline security requirements for their use. In a survey of eleven other AAU institutions conducted by our office of institutional research, we found that we were taking a more proactive stance by providing a university site license for anti-virus protection, scanning for vulnerabilities, blocking selected ports, providing private address space for the residence halls, a virtual private network (VPN) for off campus use, creating a website for technical updates, communicating advisories through internal listservs, and removing equipment from the network that serve as attack agents. We were able to accomplish these activities through the reallocation of resources and by using IP&S Loop as a decision support tool.

The universities who can demonstrate that they understand the importance of the "value added" of security will be the winners in the long run.

References

1. Educause. "Higher Education Contribution to National Strategy to Secure Cyberspace," URL: http://www.educause.edu/asp/doclib/subject_docs.asp?Term_ID=568 (July 2002)
2. Educause, p. 13
3. MindSim Corporation. "OODA Loop" URL: http://www.mindsim.com/MindSim/Corporate/OODA.html (2000)
4. Farrell, Adrian. "An Organisational Intelligence Framework for the Agile Corporation" URL: http://www.worksys.com/agile.htm (June 26, 2002)
5. MindSim, p.1
6. MindSim, p.1
7. MindSim, p.2
8. Bahadur, Gary. "Why Should You Enforce a Network Security Policy," URL: http://www.usenix.org/publications/login/2000-12/index.html (December 2000)
9. Osborne, LTC William B., Bethel, MAJ Scott A., Chew, MAJ Nolen R., Nostrand, MAJ Philip M., Whitehead, MAJ YuLin G. "Information Operations: A New War-Fighting Capability" URL: http://www.au.af.mil/au/2025/volume3/chap02/v3c2-1.htm (August 1996)
10. Mogul, Rich. "Prioritizing Security Efforts: Create Structure from Disorder," URL: http://www.gartnerg2.com/research/rpt-0102-0019.asp (January 2002)
11. Osborne, Chapter 2, p. 1
12. GAO. "Executive Guide Information Security Management, Learning from Leading Organizations," URL: http://www.gao.gov/special.pubs/infosec.guide/ (May 1998)
13. Farrell, p. 1

14. MindSim, p. 1
15. Culp, Scott. "The Ten Immutable Laws of Security Administration," URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10salaws.asp (November 2000)

Additional References

1. Dunigan, Tom, Hinkel. Greg, "Intrusion Detection and Intrusion Prevention on a Large Network. A Case Study." URL: http://ww.usenix.org/(1999)
2. Genusa, Angela. "12 Keys For Locking Up Tight, URL: http://www.cio.com/archive/030101/keys.html (March 1, 2002)
3. Northcutt, Steven. The SANS Institute, "Computer Security Incident Handling Step by Step Version 2.2," URL: http://store.sans.org/store_category.php?category=consguides (October 2001)
4. Security Director's Report. Issue 02-5. URL: http://www.ioma.com (May 2002)