The Importance of Computer Network Incident Reporting within the Defense in Depth

Adam Straub

May 2001

Version 1.2d

Introduction

"Information, information processing, and communications networks are at the core of every military activity. Throughout history, military leaders have regarded information superiority as a key enabler of victory" (Joint Vision 2020, 2000). Throughout history, information has been the key to success for businesses, countries, and militaries. Along with the vital nature of information has been the struggle to assure not only the information but also the method in which the information is secured. The rapid growth and acceptance of the Internet has made it the key enabler for exchanging information. Many organizations have become dependent on their information systems (IS) tied to the Internet such as email, websites, and the countless other forms of electronic exchange. The United States (US) Department of Defense (DoD) is an organization that is dependent on its information systems.

In order to assure its information assets the DoD adopted an Information Assurance (IA) posture designated to protect and defend its electronic information and information systems' integrity, availability, authentication, confidentiality, and non-repudiation (NSTISSI No. 4009, 1999). IA encompasses protection, detection, and reaction capabilities for computer networks.

In order to achieve Information Assurance the DoD has adopted the Defense in Depth strategy. The defense in depth has three components: people, operations, and technology, and can be compared to a medieval castle, with successive layers of mutually supporting protection, detection, and reaction capabilities (Woodward, 2000). This strategy gives the DoD information assurance community a starting point for developing effective security for the systems they are charged to protect.

Understanding the defense in depth model is far easier than implementing an effective defense in depth strategy for DoD's computer networks. The diversity of the DoD's computer networks; the constant turnover of uniformed, civilian, and contractor personnel; the rapid evolution of technology; the tightening of budgets; the growing sophistication of threat actors; and the ever-increasing demands of operational requirements creates an overwhelming complexity that inevitably leads to system vulnerabilities. The challenge that faces the IA community consisting of system administrations (SA), network managers (NM), information systems security officers (ISSO), information systems security managers (ISSM), designated approving authorities (DAA), certification and accreditation (C&A) personnel, computer network defense (CND) personnel, computer emergency response team (CERT) members, IA policy personnel, and other information security (INFOSEC) and IA personnel is where and how to most effectively prioritize the available resources of personnel and technology to support the mission. Providing 100% security is not possible, thus a risk management approach must be taken (GIAC, 2001). The result is an attempt to mitigate risk that is determined by identifying the threats and the vulnerabilities to a system and weighting these factors against operational requirements.

Businesses measure risk by determining the monetary value of the information that must be protected and can often use cost-benefit analysis to assist their decision making process for investment in computer network security applications. This means that if a company's information were valued at $100,000 then it would make little sense to spend $200,000 securing the information. The DoD and other government agencies can rarely determine a financial value for information, and therefore must measure the value of information according to the perceived harm its loss or compromise would cause.

Defense in Depth

The DoD, like most large modern organizations, has become dependent upon its information systems, specifically its Internet Protocol (IP) networks. This dependence has created vulnerabilities that must be actively managed to prevent the theft, corruption, or destruction of sensitive national security information. The widely accepted defense in depth model provides an understandable framework for protection, detection, and reaction.

The DoD has identified four specific layers for a defense in depth. The layers are: (1) host or end user systems; (2) enclaves and the enclave boundary; typically a local area network (LAN); (3) networks that link the enclaves, typically wide area networks; and (4) supporting infrastructures, which are typically the cryptographic solutions like public key infrastructure (PKI) (Joint Chiefs of Staff, 2001).

There are many commercial and government tools available that provide protection, detection, reaction, and recovery capabilities such as: firewalls, intrusion detection systems, anti-virus software, network/enterprise management tools, and backup devices. The defense in depth strategy provides IA and security personnel a common framework in which to develop a defense in depth for their unique organizations. The people tasked with assuring the information and information systems employ the technologies in an operational context that is appropriate for the organization; thus, the key components of the defense in depth are: people, technology, and operations (Woodward, 2000). What complicates matters for IA professionals are varying standards and expectations created by personnel that understand operational issues, but may not completely grasp the intricacies of IP networks.

DoD Environment

Understanding the environment of the military is critical to understanding computer network defense issues. Within the DoD, there are different functional disciplines such as: personnel, intelligence, operations, logistics, and communications. The purpose of the DoD/United States Military is to fight and win the country’s wars. This fundamental purpose creates the relationships between the functional communities. The operations community consists of the commanders and leaders who are ultimately responsible. The operations community is the chain of command. All the other functional communities support the operations community. There are times that the support relationships become clouded, but as an issue is raised, the communicator, or personnelist, or intelligence officer will defer to the operational commander. Acknowledging that this is a gross over-simplification of the DoD functional community relationships, this depiction provides a baseline understanding. This relationship is often referred to as supporting the warfighter.

The communications community typically manages the DoD computer networks. Generally speaking, the communications community is the functional expert when it comes to all computer related matters. As the DoD has become increasingly dependent on its computer networks, the other communities began to recognize the roles their disciples played within computer networks.

During the 2000 Congressional Hearings on Information Superiority and Information Assurance, Mr. Art Money, the Assistant Secretary of Defense for C3I (ASD/C3I) spoke of the fragile advantage the DoD has in information capabilities, and how the DoD's systems that collect, process, and disseminate information are vulnerable. In order to maintain the US's advantage more robust capabilities and processes are required.

Computer Network Incident Reporting

A specific issue that the DoD is struggling with is its reporting procedures for computer network incidents. Computer network detection capabilities are rapidly progressing but are far from mature technology especially within the DoD. Many command and installations have deployed intrusion detection systems (IDS) such as RealSecure, Snort, and TCPdump on their networks. The Defense Information Systems Agency (DISA) has deployed Joint Intrusion Detection Systems (JIDS), throughout much of the DoD's networks providing DISA with an enterprise system for intrusion detection.

The data that these sensors are collecting is providing a much greater awareness that there is a serious cyber-threat that challenges the DoD's networks on a daily basis. It is at this juncture that the DoD is struggling to refine the processes involved with computer network incident reporting. The DoD has two issues that generate debate when in comes to computer network incident reporting. The first issue is what to report and the second issue is who to report too.

What to Report

The DoD has defined seven categories of computer network incidents specifically: category 1 – successful root access, category 2- successful user access, category 3- failed access attempt, category 4 – denial of service attack (to include distributed denial of service attacks), category 5 – poor security practices, category 6 – malicious logic such as viruses, worms, Trojan horses, and logic bombs, and category 7 – probes which are further defined into three sub categories of serious (more than three sites and or services impacted), significant (1 to 3 sites and or services), and simple (one site one service).

These definitions are good and are generally easily understood. What is missing is the explanation of how the specific IDS register one of these types of computer network incidents. A trap that some computer network defense personnel have fallen into is reporting consistently decreasing numbers of events. The operations personnel assume that since there are fewer incidents this month than last month then the computer network security must be getting better. This is a false sense of security that not only creates a misperception but it is also the road to the steady decline of the organization's IA budget.

As with all computer network devices, configuration control is the key. When an IDS is initially installed there are all kinds of false positives generated. It takes the analyst some time to figure out what alarms are valid and what alarms they should turn off. The time varies based on all the other responsibilities the analyst has, which the new IDS system administration is typically in addition to the individual's system administration or network management responsibilities. In the meantime, the IDS is logging thousands of events on the network, which the analyst is obligated to report. As the analyst slowly learns what alarms are false and begins to refine the rule set the number of "reported" incidents decline. The result as mentioned earlier is a false sense of security. To confuse the situation further, the results from one IDS are compared to the results from another IDS at a different installation. Invariably the two IDS servers have dramatically different results over identical time periods. Again, this is the result of only different rule sets and configuration management.

Avoiding this trap is important for IA professionals in order to maintain credibility and the favor of the person who controls the purse strings of an organization. IA professionals can succeed in this endeavor by being deliberate in their configuration control of the IDS, educating the operations personnel, and recognizing that this scenario will likely occur when implementing a new IDS product.

Who to Report Too

CJCSI 6510.01B defines organizational reporting procedures with a tiered approach, of local to regional/service to global. Organizations are obligated to report all computer network incidents. CJCSI 6510.01B defines specific time periods in which different categories of incidents must be reported to the highest level. This expectation is unrealistic in that the reporting organization has no control/authority to report beyond their higher headquarters in order to ensure the incident is received at the highest level, being the DISA Global Network Operations and Security Center (GNOSC). Additionally organizations are expected to simultaneously report up their respective service chains and to the regional DISA field office. Figure 1 depicts the overall incident reporting structure.

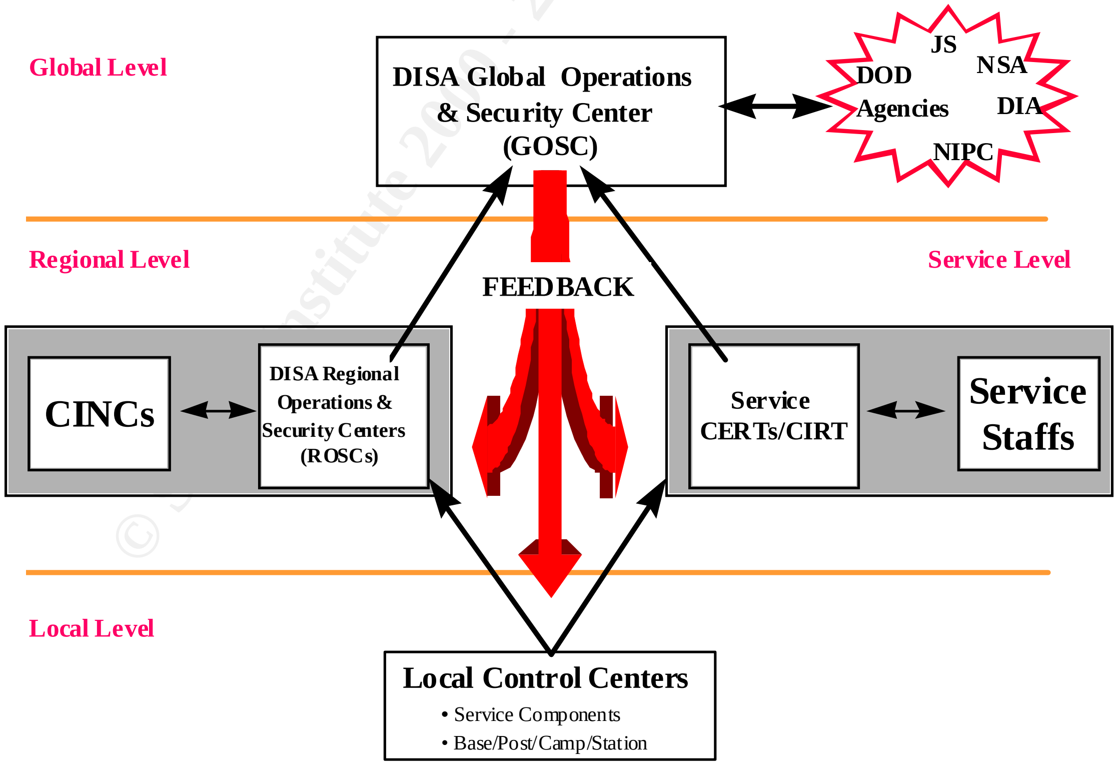

Figure 1. DoD Computer Network Incident Reporting Procedures

This dual reporting procedure is not the issue. What becomes the issue are the downward directed actions that many commands are given that conflict and the multiple redundant analyses that are conducted at the different levels based on intelligence, operational impact, and the incident technique.

An army installation may have had an incident, and it reported the incident appropriately through both reporting chains. The follow-on reporting expectations become burdensome to the army installation when the Army Computer Emergency Response Team (CERT) requests/directs that certain procedures occur while the regional NOSC, receiving instruction from the geographic command authority, request/direct additional or different procedures. Figure 1 is missing the downward arrows that inevitably follow the initial reporting of an incident, and the corresponding return arrows that provide the additional clarity and explanation that each organization desires.

The way to alleviate these multiple follow-on requirements is to have a shared view of computer network activity. With a shared view, the regional and global level organizations would have all the data that the local level organization has. This shared view equates to an Information Assurance Common Operational Picture (IA COP), that provides IA situational awareness to not only the local level, but to also, the regional and global level organizations. Some tools show promise in providing an IA COP. DISA uses the Integrated Network Management System (INMS) to provide network-monitoring capability. Another emerging tool is the Automated Intrusion Detection Environment (AIDE), which correlates IDS, firewall, router, and other network monitoring devices outputs to provide a version of an IA COP.

Additional redundancy occurs when each organization analyses the incident. The local organization assesses the operational impact, as does the regional organization. The regional and global organizations analyses the intelligence impact. All three levels analyze the incident technique. When any of these analyses conflicted, there was confusion as to which origination's analysis, and resulting recommend should be followed. The DoD appears to be improving in this arena in that it is consolidating its computer network operations under a single command the Joint Task Force – Computer Network Operations (JTF-CNO). JTF-CNO will likely be the settler of disputes, and given time should become the respected authority on computer network operations.

Conclusion

The DoD, like most large modern organizations, has become dependent upon its computer networks. This dependence has created vulnerabilities that must be actively managed to prevent the theft, corruption, or destruction of sensitive national security information. The DoD has adopted the defense in depth strategy whose components of people, technology, and operations provide an understandable framework for protection, detection, and reaction capabilities.

Employing Information Assurance through a Defense in Depth strategy based on the premise that protection is not 100% secure, and that a detection capability the will allow the DoD to rapidly react to computer network incidents. Ensuring that the immature technology of intrusion detection is not misunderstood as it is implemented will prevent the DoD from falling into a false sense of security when the nation's technology advantage is so fragile. Developing an IA common operational picture will streamline reporting procedures, increase responsiveness, and heighten computer network situational awareness. By continuing to refine processes for identifying, reporting, and responding to computer network incidents, the DoD can achieve the information superiority described in Joint Vision 2010 and deliver the full spectrum dominance described in Joint Vision 2020.

References

Global Incident Analysis Center. (2001, February). Information security highlights. Presented during the Kickstart Track: Information Security K-1, for the Systems Administration, Networking, and Security (SANS) Institute, Honolulu, HI.

Joint Chiefs of Staff (2001, March). Information assurance (defense-in-depth). (CJCSM Final Draft 6510.01). Washington, DC: Author.

Joint Chiefs of Staff (1998, August). Defense information operations implementation. (CJCSI 6510.01B). Washington, DC: Author. http://www.c3i.osd.mil/org/sio/ia/diap2/

Joint Vision 2020. (2000). U.S. Dept. of Defense, The Joint Staff, Joint Electronic Library http://www.dtic.mil/jv2020/index.html

Money, Arthur L. (2000, March). 2000 Congressional Hearings on Information Superiority and Information Assurance - House Military Readiness and Military Research & Development Subcommittees http://fas.org/irp/congress/2000_hr/00-03-08money.htm

NSTISSI No. 4009. (1999, January). National Information Systems Security (INFOSEC) Glossary. http://constitution.ncsc.mil/wws/nstissc/Assets/pdf/4009.pdf

Woodward, J. (2000, February). Information assurance through defense in depth [Brochure]. Washington, DC: Joint Chiefs of Staff.