Global Information Assurance Certification Paper

The Need for Operational Defense of Information System Networks (ODIN)

Timothy M. Read

February 13, 2001

Introduction

In just the time it takes to read this paragraph it is possible that somewhere in the world an information system has come under attack. This sounds cliché, however the threat is real and it is global in nature. The attack could be methodical, it could be a coordinated strike, it may be a disgruntled co-worker seeking revenge, or it could simply be your pal opening an email attachment containing a virus that has begun working its way through "your" network -perhaps its name is Anna this time. Chances are that this attack or its damage will go unnoticed for awhile. According to a recent article in *Internetweek*, distributed denial of service attacks and automated scans for specific vulnerabilities have become a real problem. Hackers are scanning ports en masse, coordinated attacks are gaining popularity and network users who appear to be valid users may be imposters. Meanwhile, it should also be noted that some industry estimates postulate that 60 to 70 percent of attacks come from inside the company.[1] The question is not where or even when will the next attack occur; rather the question is how long will the attack go unnoticed, uncontrolled and what will the damage be?

Eugene Spafford of Purdue University, the well-respected security visionary, recently stated "the security landscape, with viruses, malicious hackers and insecure system designs, is going to get worse, and the problem is human nature not shortfalls in technology."[2] The QAZ worm for example, was used to break into Microsoft last October to steal corporate secrets. Hackers gained access to 15,700 customer accounts, including credit card information.[3] There is still some debate over how long the QAZ worm operated undetected. It is a commonly held belief that ignorance of the worm enabled hackers to collect much information. Denial of service (DoS) attacks are a real problem and are occurring almost daily against major Internet companies such as eBay, CNN, or Yahoo for example.

Security is more than implementation of intrusion detection systems (IDS), firewalls, and passwords protecting computer accounts. This paper explores the need to "operationalize" the defense of information system networks (ODIN), and proposes an ODIN methodology for security policy makers. It considers the threat of intrusion and other security risks to information system networks and the inability of the business and industry to effectively monitor and defend against these threats. It also discusses weaknesses in contemporary security practices, and concludes with a model framework for the implementation of ODIN which executives, managers, and information technology professionals may all understand and agree on equally.

Contemporary Information System and Network Security Operations

System security today is not proactive. Security is reactionary and response driven, after all, the future cannot be predicted. The trouble is that system/network threats are too numerous and far too lethal to ignore today. Complacency often works its way inside organizations and

security can become sloppy. The opposite end of the security spectrum is rampant paranoia. Striking a balanced security posture is critical for effective information operations. A proactive balance involves the interaction among users, management, and among IT professionals.

The term *operational defense* means to make IT professionals, practices and procedures of proactive in nature. Operationalizing the defense of information systems and networks then, suggests that a dedicated network / system administration security specialist or a team of specialists is actively monitoring and defending the networked systems in the organization. The demand for such a position within the organization is often thought of, yet seldom implemented.

Business organizations will often hire a security expert, or security officer to fill a void existing within the organization. Yet experts filling these positions often fail to achieve security objectives because they are usually made accountable to an overwhelming array of security challenges, large job responsibility and the daunting task to formulate and implement strategic security management. Those security experts considered to be effective within organizations may develop security policies, practices or procedures for their organizations, but fall short of implementing active security programs. Exceptional security officers might incorporate security into the organization by way of change management, and will budget for purchases and implementation of security software, technical training or other technical security solutions. In the past, the IT department had become the de facto security experts and assumed security responsibilities in addition to supporting users and managers on a daily basis. The security officer however, is seldom responsible for the day-to-day, hands-on, active monitoring and proactive or reactive security for a system or network, but he or she should be.

Contemporary security often relies on semi-automated intrusion detection systems (IDS), anti-virus software, network port scanning auditing software and outsourcing of security solutions is how an organization attempts to mitigate IT/IS risk. Few IT security operations include a dedicated staff of security professionals who work explicitly for the defense of the network. Security sometimes becomes a euphemism for the hopeful adherence to an organization's written security policies, procedures, and practices; and often contains a healthy mixture of scripts, commercial security software and the occasional outsourcing of security analysis. The problem is that each of these defensive measures requires a busy administrator to read software generated reports, logs, and alarms in order to confirm what is already suspected, the network is at risk and has possibly been attacked.

Information Assurance

The objective of operational security is information assurance. Information assurance consists of safeguarding systems confidentiality, maintaining data integrity and guaranteeing system/application availability to users 24 hours a day, seven days a week. Basic security implementation consists of consistent and effective enforcement of countermeasures designed to protect the foundation of information assurance, thereby protecting the organization.

A strong system defense logically consists of multiple layers of protective measures designed to protect the organization; protect customer confidentiality; maintain system

application functionality; and to insure integrity of data. Effective information assurance guarantees information system availability for all users at all times. Operational network defense should consist of strategies, plans, tactics and implementation of security procedures designed to balance system vulnerability relative to the threat in order to mitigate system risks. The goal of operational security is about maintaining high fidelity information assurance.

Information attacks are not easily predicted nor easily identified. Consider for a moment how a doctor treats a patient. An information attack and defensive countermeasure are analogous to the treatment that a patient might receive from a doctor. A patient complains of an illness or its symptoms. The patient's vitals are screened, and the doctor conducts further testing to identify and isolate the problem. The doctor then diagnoses a problem by eliminating what the symptoms are and by what they are not. Ultimately, the doctor through a combination of trial and error, and medical knowledge, can diagnose, treat and prognosticate patient recovery. Presumably, the patient reduces workload and stress until recovery is complete.

The system /network administrator is not so lucky. Often he/she is faced with unknown information system symptoms causing the network/systems to malfunction. Additionally, the administrator does not have a lot of time to diagnose/study a problem and posit solutions because once the administrator discovers that a problem exists, he/she may already be under an attack of unknown proportion. Containment options can quickly dwindle, perhaps forcing the network to become isolated and shutdown from operations. At this point, information assurance has not only been compromised, but been denied to the user. Without an operational approach to network security "symptomatic" treatment of network ills proves costly.

Intrusion Detection Alone is Inadequate

A good IDS can effectively detect user actions within the system or network that represent symptomatic attack-style behaviors. An IDS is effective in monitoring disturbances or disturbing actions over the information system network. An IDS alone, does not guarantee information assurance across the board of operations; furthermore an IDS requires that someone be monitor the system and read logs. Moreover, and IDS can detect only the vulnerability patterns it was designed to detect. Because an IDS is responsible for identifying and categorizing vulnerability checks, an IDS may report falsely. False positive reports are frequently issued because an IDS lacks data to absolutely confirm or deny the vulnerability. The IDS simply guesses and errs on the side of caution. This can create additional work for security.

An IS network cannot effectively communicate its health -its status of operational readiness to the administrator the way a patient can communicate it ills to a doctor. According to Ryon Packer of Instrusion.com and IDS vendor, "Intrusion detection is reactive. People buy tools after the attack similar to the way they buy firewalls."[4] IDS in and of itself, is not an active defensive layer, or an operational defense. Someone must also actively monitor network activities.

Perimeter security devices such as firewalls or a demilitarized zone are effective countermeasures when employed to defend against the threat of outside "unwanteds" from gaining access to your networked systems. Firewalls can reduce the volume of people gaining

access to your site and represent the guardians at the gate, so to speak. Firewalls can be penetrated and should be thought of as merely another layer of an organization's defensive posture. System managed defenses alone will not guarantee information assurance.

The operational defensive approach incorporates a combination of automated, preventative security countermeasures and active human monitoring and a continuous evaluation of the status of networked systems. A strong layered defense consisting of implementation of anti-virus software, firewalls, DMZs, IDSs, port scanning is essential; however the strong suit of operational defense is the service provided by a dedicated and well-organized IT professional who monitors users, trouble areas, and network responsiveness. "Operationalizing" the defense of your network takes IT security beyond symptomatic treatment, and prescribes preventative treatment for the IT environment.

Security -Supporting the Operational Environment

The IT environment functions to support the goals, requirements and operations of the organization. Managers have responsibility to the organization to ensure that their department/division and/or functional areas are meeting those goals as well. Users who report to managers, levy support requirements against system/network administrators. System and network administrators of course, are often responsible to users, managers and each other to ensure that the organization's IT demands are responsive and fully functional. Securing systems and supporting the operational environment of the organization, its goals, its users, and management is the purpose of information systems and the network. Operational Defense of Information System Network model considers the organization first. At the heart of the Operational Defense of Information System Network model is IT professionals' buy-in to the goals and operations of the organization. The ODIN model demands that the IT professional recognizes his/her job responsibility, assumption of task ownership within the IT infrastructure and that he/she recognizes team play as being tantamount to protecting the integrity of the network systems -information assurance. The IT professional must also recognize that information systems support information operations and communication within the organization. Communication is simultaneously horizontal and vertical within the organization. Information systems support the organization's mission along both divisional and functional lines.

The goal of an operational IT professional is to recognize that his/her actions will directly affect the readiness, security and efficiency in information operations. When a user needs an application and it cannot be accessed, the IT security professional has failed the organization, even if it is not his/her fault directly. Therefore, the network and every system within the network must be continuously monitored, protected and maintained. The IT security professional therefore, must recognize that monitoring all system operations and maintaining a healthy system is his/her first and last priority.

Operational Defensive Security -Cyclical in Nature

Operational defense oriented information security is a conceptual, diligent and cyclical process. The information security professional must be thinking about physical threats to the

entire organization, ranging from remote users sitting outside of the edge of the network to the application layer within the organization. They must also consider the physical barriers within the operating facility or facilities, the logical threats relevant to information assurance and they must continuously strive to mitigate all risk areas potentially affecting the organization. In this sense it is both a philosophical practice and cyclical in nature. The operational defense of information system networks model has five distinct phases: Evaluation; Planning; Implementation; Monitoring and Reevaluation.

Evaluation, is the first step toward implementing an operational defense, it is designed to recognize all physical and system vulnerabilities. The IT security professional and organization practicing operation defensive security must conduct a vulnerability assessment of the entire organization. The vulnerability assessment should include a thorough review of the entire organization from an IT perspective and from an operations (management and user) perspective. It will include more than a system/network and infrastructure vulnerability assessment. It must also include an assessment of the state of the physical security of the organization's facilities, and it should consider the implementation of logical security controls for IS operations. The evaluation should also include a thorough review of all IT policies, user documentation, network flowcharts, operational process flowcharts, system recovery plans and relevant managerial policies. The evaluation is a cross-functional assessment, as it considers the effectiveness of the IT infrastructure to the organization's operations on a department by department basis.

The next phase is the Planning phase of the ODIN model. The planning phase is designed to remove as many of the organization's vulnerabilities as possible given the financial, operational and personnel limitations in place within the organization. In this phase documentation, policies, organizational changes, job responsibilities and technical solutions are defined. The organization reviews the findings of the evaluation and attempts to tackle each of them thoroughly. This is also the phase where the IT department can obtain management buy-in to technical problems and risks that may have been plaguing the organization for some time. Short-term strategies, standard operating procedures, and job descriptions should be devised.

It is in this phase where the IT department should be made "operational" in nature. Operationalization is achieved when defensive security practices are identified to support the organization's operations. IT security professional responsibilities will be clearly defined according to their traditional IT administrative responsibilities. IT professionals will devise plans to monitor their own areas in an effort to establish network/system behavioral patterns. Network administrators for example, might be assigned to monitoring duties, or port scanning responsibilities that had been overlooked in the past; or systems administrators might start monitoring user account activity logs and establish help desk operations to actively support users.

Once management has achieved an understanding of the vulnerabilities, a strategic risk mitigation plan must be presented for management approval. This plan too, must be effectively communicated to management. It should contain a detailed description of the threat, and the impact to the organization in terms of risk. This plan should not be thought of as being "the master attack plan," rather it should be noted that this plan will continuously change as will the

state of your systems and network over time. The plan should be designed to fix those areas according to risk prioritization and cost effectiveness.

Phase three, the Implementation Phase is designed to efficiently implement operational defensive security. The Implementation Phase is perhaps the trickiest phase as this is the phase in which the risk mitigation plan and all operational security measures are put into operation. Initially, growing pains will confront all personnel within the organization. Personnel will begin to perform operational duties in accordance with documented call out procedures, and follow established policies and practices. Documentation is critical for successful implementation of all operational defensive programs.

Phase four, the Monitoring Phase serves to reinforce the importance of security programs and practices that were instituted during the Implementation Phase. Monitoring is simply that. IT security professionals will perform daily operational security functions, hold impromptu meetings for information sharing, or conduct change over meetings during shift change to insure that counterparts are quickly brought up to speed on key issues. The monitoring phase will consist of daily activities such as the review of automated intrusion detection system logs, user account logs, network scanning logs, data backup recovery logs, or unusual help desk trouble shooting logs. The monitoring phase is a daily event and all key information items should be noted and recorded for further discussion.

The final phase, the Reevaluation Phase is critical to improvement of operational defensive security practices. The monitoring phase shall begin as directed by the organization. A good starting place is a quarterly review. At this time, the IT Director shall conduct a "hot wash" review of all critical defensive security events -success, failure and interesting security trends. The Reevaluation is a critical review of all processes that have been implemented and it will summarize those practices that are working well and those that need to be finely tuned, fixed, or eliminated based on an acceptable level of organizational risk. The IT Director should communicate the quarterly findings to the organization's management and a new period of evaluation (phase one) should begin again based on strategic management's guidance. The cycle begins again and an operational defensive structure is reinforced within the organization.

The Future of Information Defense -Software and Hardware

While the future of information defense/security continues to become more and more automated to assist network security, it will still require the human touch and operational implementation within the OSI model. In a recent article written by Lisa Morgan appearing in *Internetweek* Avi Fogel, CEO of Network One an IDS vendor, summarized vulnerability:

> The objective (of security and IDSs) is to minimize vulnerability. Ideally, you could find a more generic tool that prevents classes of intrusion like Trojan horses. A tool like that could have prevented the recent Microsoft break-in (QAZ, in which an employee's machine was compromised).[5]

Morgan further communicates that many IDS and firewall vendors are marketing systems that monitor the higher-level layers beginning at the Network and Transport Layer (3 & 4) and

targeting the Applications Layer (7). Layer 7, is typically the popular location for embedding of malicious code. Companies are now developing intrusion detection systems that monitor the edge of a network so that the host can observe attacks that may be directed at it. Monitoring traffic types, attack patterns and putting up defensive barriers at these layers aims to deny hacker success and pushes the hacker threat out far enough from the organization to reduce the risk of intrusion that might be obtained via social engineering attacks. This treatment highlights the need to establish operationally aligned defensive layers which restrict network access, access to sub-networks, network services, storage and applications operating within the internal network of an organization.

In conjunction with advances in security software applications, managed security monitoring has become the rage during 2000. Outsourcing of security monitoring operations has become a prosperous industry. Riptech, a security monitoring and professional services firm has grossed approximately $23 million in funding and supports over 100 clients globally. In fact, IDC predicts that the U.S. market alone for security consulting, implementation, management and training services will leap to $8.2 million in 2004, up from $2.8 billion in 1999.[6] Outsourcing has become popular for a whole host of reasons, most of which extend beyond the scope of this paper. However, foremost among these reasons is the demand for cost-effective and efficient protective security services. Management in most organizations would rather pay for this service than build it from square one within the organization.

In addition to security outsourcing, a recent study in January 2001, assessed that the worldwide security software market is expected to grow at a compound rate of 21.7% through the 2004 period.[7] Not only will demand for IT network security continue to grow, so too will the requirement for organizations to spend time, money and resources just to stay abreast of the software security industry's best software. Organizations who plan, organize, equip and implement operational security practices now will perform better in tomorrow's environment than those who fail to deal with security today.

Implementing the ODIN Cycle

The table below contains the model for the ODIN Cycle. The table can be used as a model for IT managers and professionals to efficiently achieve an operational defensive posture for their organization. The table is representative of many practices commonly outlined by information system auditing techniques. The measurable actions associated with each phase of the cycle are commonly called out within various industry certification programs; however the real value of each of these practices is recognized only when the activities are made operational by an organization. The value the ODIN model provides to security is its cyclical implementation of each process phase. Thus the goal of ODIN is to seek continuous and measurable improvements of security practices supporting an organization's operations.

	Cycle Phase	Measurable Actions of Each Phase
1.	Evaluation	Communicate with management in all IT supported departments about the forthcoming evaluation. Develop and provide a questionnaire to

managers that asks managers to evaluate how effectively information systems, security practices and the existing network supports the goals of the organization.

Conduct the IT Security Assessment for all information systems in use by all users within the organization

- Document & Inventory All Systems in use within the Organization
- Document flowcharts for the information processes supported by information systems
- Assess the Network Infrastructure and Network Design
- Document Flowcharts for the Existing Network Architecture Including the Infrastructure
- Review and inventory all hardware
- Review and inventory all software in use on all machines
- Review Existing IT Policies; Identify shortfalls
- Review Existing IT Strategy and consider how it supports operations
- Review IS Standard Operating Procedures
- Review User Policies
- Review IT Administrative Policies
- Review IT Job Descriptions and IT Job Functions
- Create and document New IT Job Descriptions
- Review Existing Call Out Procedures (Checklists) and update them
- Review Physical Security to the IT Area
- Review Logical Security among Systems and Over the Network

2. Planning
   - Review existing gaps and design the "Get Well Plan"
   - Establish IT Policy and Standard Operating Procedures for the Organization
   - Establish an Active Network Monitoring Department and integrate Configuration Management
   - Establish Explicit and Specific Job Descriptions for all IT professionals that correspond to the organization's operations
   - Establish Call Out Procedures for Each IT Responsibility and Activity
   - Coordinate Change Management with Operational and Strategic Growth of the organization
   - Obtain Management Buy-in
   - Assign Duties and Develop a Time Line

3. Implementation
   Begin implementing the "Get Well Plan"
   - Assign Duties
   - Obey policies
   - Implement strategies
   - Carry out call out procedures and defensive practices

4. Monitoring — Begin diligent monitoring practices of organization's information systems and network
   - Establish Help Desk Operations
   - Audit user accounts, the network and review monitoring logs
   - Communicate with other organizational department such as Human Resources to track new/terminated employees and monitor those accounts
   - Update inventories and configuration changes
   - Monitor system reports, trouble tickets, help desk calls
   - Conduct change over briefings at shift change
   - Review Data Backup & Recovery logs
   - Periodically test emergency back up procedures
   - Have IT Security Professionals keep logs and monitor and report trends
   - Conduct periodic meetings covering unusual security / operations topics

5. Reevaluation — IT Director kicks off "hot wash" review of quarterly events
   - Obtain high interest items lists, reports and trends from each IT department area (network managers, system administrators, application administrators, change managers, email administrators, database administrators, etc)
   - IT Director documents findings
   - IT Director communicates self-assessment findings, pros, cons and significant events to management, users and IT personnel
   - IT Director prepares for next high level evaluation period
   - Cycle continues

Conclusion

While the market for security software will continue to rise in demand, so too will the demand rise for well-trained and operationally oriented information technology professionals. In response to last year's increase in cyber attacks, nineteen of the IT industry's leading companies have banded together to form the IT-Information Sharing And Analysis Center. This new organization was created in January 2001 to facilitate the sharing of threat and vulnerability information.[8] Industry has recognized that information sharing and human interaction is the best response method for tracking and countering threats to information systems. Operationally oriented defensive security, continuous monitoring and self-improvement practices will mitigate much IT risk and keep organizations operating when others fail.

---

[1] Morgan, Lisa. "Be Afraid...Be Very Afraid -- Malicious attacks are on the rise, and trends are harder to predict-step one is admitting your company is vulnerable." *Internetweek*. Manhasset. Issue 843. Page 37. ISSN 10969969.

URL: http://www.internetwk.com Search on Network security.

[2] Zuckerman, M.J. "Eugene Spafford Security Visionary." *USA Today.com*. Final Edition. Arlington, VA. December 28, 2000. Page D.3. ISSN 07347456.
URL: http://www.usatoday.com/.

[3] Morgan, Lisa. "Be Afraid...Be Very Afraid -- Malicious attacks are on the rise, and trends are harder to predict-step one is admitting your company is vulnerable."
Internetweek. Manhasset. Issue 843. Page 37. ISSN 10969969.
URL: http://www.internetwk.com Search on Network security.

[4] Morgan, Lisa. "Be Afraid...Be Very Afraid -- Malicious attacks are on the rise, and trends are harder to predict-step one is admitting your company is vulnerable."
Internetweek. Manhasset. Issue 843. Page 37. ISSN 10969969.
URL: http://www.internetwk.com Search on Network security.

[5] Morgan, Lisa. "Be Afraid...Be Very Afraid -- Malicious attacks are on the rise, and trends are harder to predict-step one is admitting your company is vulnerable."
Internetweek. Manhasset. Issue 843. Page 37. ISSN 10969969.
URL: http://www.internetwk.com Search on Network security.

[6] Savage, Marcia. "Security takes front seat." *Computer Reseller News*. Manhasset. January 8, 2001. Issue 927. Page 41. ISSN 08938377. URL: http://proquest.umi.com/pqdweb/ Search for network security on Proquest database online.

[7] Technical Editor. "Security Software Market Set to Grow." *Netimperative*, January 16, 2001.
URL: http://www.netimperative.com/technology/newsarticle.asp?ArticleID
=7513&ChannelID=3ArticleType=1

[8] Business Editors/HighTech Writers, "High-Tech Industry Announces New Information Sharing and Analysis Center for Information Security Center to Establish Unprecedented Level of Industry Cooperation on InfoSec Issues." *Business Wire*. BW2673. January 16, 2001.
URL: http://www.businesswire.com/webbox/bw.011601/210162673.htm