ADAPTIVE NETWORK SECURITY HANDBOOK

Preface

This document describes the general risk conditions associated with the world's networked systems, presents specific problems and challenges, and defines a recommended solution approach. This paper also addresses the need for the solidification and global acceptance of highly essential network security processes, standards, and support products. The primary goal is to provide the reader with a solid foundation, and/or approach, from which to build an internal, site-specific, end-to-end security program.

This paper raises the reader above the proverbial trees associated with network operations and security in order to allow for a clear view of the forest, that is, the Big Picture. It takes the reader back far enough to allow them to take a breath and a clear look at what is really wrong so they can plan for and migrate to a standardized security model supported by rigorous, traceable processes that provide sound, repeatable, and cost-effective solutions.

In short, the paper outlines the need and basic structure for an *Adaptive Security Model*: a model supported by well-defined underlying processes, appropriately trained personnel, and an effective, value-added toolset.

The processes, models, and automated approaches defined within this paper expand upon many cutting-edge solution approaches and models either implemented or under study by world leaders.

Tom Noonan
President and CEO, ISS

For questions or comments regarding this Adaptive Network Security handbook, or any other concepts you would like to discuss with members of the ISS staff, please contact the following Primary Authors and Network Security Professionals at (800) 776-2362:

Chris Klaus (Founder and Chief Technical Officer)
Patrick Taylor (Director, Strategic Marketing)
Jeffrey Z. Johnson (National Director of Strategy and Operational Services)

Adaptive Security

THE PROBLEM IS SERIOUS!

As represented within Figure 1, traditional security activity (i.e., activity associated with physical security) is fairly static. There is a valid sense of normalcy. Over the past ten years, there has been very little change in terms of overall activity levels and organizational impact. The field is well understood, adequate controls and metrics are in place, and since it is measurable it can be improved upon when and where necessary. The trends represented within Figure 1 provide a consolidated interpretation of many of the threat and incident studies provided over the past two years. As one might guess, the computer security domain is so new that it has yet to reach a point that allows us to define normal and abnormal. In many ways it is completely out of control – the Wild West of the 21st century. The Wild West had Billy the Kid, the James Brothers, Butch Cassidy and the Sundance Kid. Today we hear about cyber-outlaws such as Kevin Mitnik, Erik Bloodaxe, Agent Steal, Lex Luther, and Phiber Optik. There are very few laws, and even if the laws were in place, the processes and technology are not yet standardized and implemented in a manner that supports consistent or adequate enforcement of such laws. In addition to this, these outlaws are, in many ways, *invisible*. They can move around without being seen or making a sound. That is, if they're allowed to.

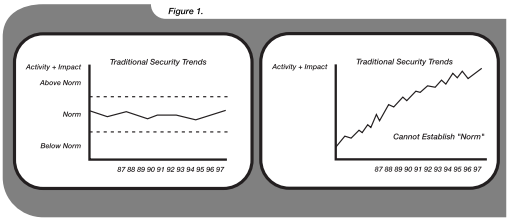

Figure 1. The Computer Security Domain Is Out of Control

Who has not imagined what it would be like to be invisible? Being able to go wherever you wish and do almost anything you wanted without fear of detection and apprehension is almost too much to comprehend. What would you do? Where would you go? Would you be able to control your lust for self-fulfillment, or would you give in to temptation and cross the lines of civility and ethics? Life as a hacker, cracker, phreaker, or the like, can be similarly parallel!

This new breed of outlaw can travel virtually unseen and unheard, gaining access to your most private and valued resources and assets. They can review your e-mail, sensitive marketing plans, budgetary data, or even electronically transfer your financial assets to their off-shore accounts. Always remaining just out of reach of apprehension and prosecution. All of this can be done in about the same amount of time it would take the Network Security Officer to print and review a typical daily audit log. Cyberspace outlaws can pull the equivalent of an entire moving van up to the organizational loading dock and get away with cash, trade secrets, sensitive customer lists, or other valued assets. Conversely, they might choose to simply walk the halls of darkness, destroying equipment, files, and other valued assets. Of course, this is fantasy. This would never happen. Operational and Security Managers surely have implemented the necessary security processes, infrastructure, and resources to protect their organization and its valued assets. Or have they?

As alluded to above, organizations have implemented sound physical security processes and controls. These organizations typically implement variations of a similar risk reduction model and as a result, operate at consistently low and uniformly acceptable levels of risk. Experienced security staffs understand, and are very comfortable with, the large quantity of security-related statistics and process models. They are familiar with the type and format of the data and understand the value (return on investment) associated with defining, implementing, auditing, measuring, and improving traditional physical and/or information security programs. So in the case of physical security, these organizations are adequately addressing their risks. But the same cannot be said for the computer security field. Whether you subscribe to the belief that the field has been around for ten, 20, or even 30 years, one thing is for sure: it's far from being stable or globally understood. The rapid evolution of technology and advancement of the threat within this same period of time is unbelievable, almost intimidating. In comparison to physical security, computer security is still in its infancy. It has completely new variables and there are new twists to old variables. Just about any attempt to force the computer security program into an existing physical security model typically results in a difficult and somewhat costly realization that it just will not fit! The physical security models will need some tailoring and expanding in order to address this new domain. The new models will need to address complicated issues such as the evolving threat and vulnerability conditions, which typically are described as chaotic. These chaotic conditions are alarming to industry and government leaders, who are familiar with their critically high network interdependencies and the potential consequences associated with network exploitation. Today, almost every country in the world is highly co-dependent upon the same, or inter-connected, communications, power, transportation, and utility networks. Whether through the Internet, modems, or leased lines, almost every one of these networks can be traced to each other, and studies indicate that greater than 75% of these are highly vulnerable.

The problems associated with high vulnerability levels are magnified by the computer security field's general lack of standards and processes, the inability to develop sound policies, and the perceived inability to ensure the policies are followed. Some believe the lack of policy is the primary issue. But without some very basic, scientifically based standards, processes, and metrics in place, the policies will do little more than take up space on everyone's bookshelf. The policies associated with the computer security field must address a wide range of complex threat and vulnerability issues. And in today's computer security environment, it is difficult to locate two security or network professionals that can agree on even the most basic security definitions, let alone develop a consistent, comprehensive security policy. In addition to these issues, those responsible for computer security find it difficult to gain organizational acceptance of the severity of the problem and need for such processes. This lack of acceptance continues even though piles of relevant support data continue to accumulate. For example, a recent study conducted by WarRoom Research LLC, in support of the U.S. Senate's Permanent Subcommittee on Investigations, once more indicated alarming trends associated with its nation's risk conditions. The data within this study was not unique, nor was it the first of such a report. Over the past five years, a number of similar studies have been conducted by the following, each of which reported almost identical trends:

- FBI
- Ernst & Young LLP
- InformationWeek
- Computer Security Institute
- Government Accounting Office
- U.S. Military Services

These studies provided very clear insight into the growing problem. They indicated significant increases in the size and skill level of the threat groups, activity levels, and in the organizational impact associated with internal and external attacks. The following are some of the WarRoom Study's highlights:

The human threats are growing in numbers and sophistication.

- 61% of those organizations responding to the WarRoom Survey had experienced an internal attack within the past 12 months.
- 58% of those organizations responding to the WarRoom Survey had experienced an external attack within the past 12 months.

The vulnerability conditions associated with our networks are well known and understood.

- Worsened by the availability of hacker tools available free on the Internet.
- Over 45% of those attacks reported to WarRoom Research were associated with advanced technical hacking techniques, for example: sniffers, theft of password files, vulnerability probing/scanning, Trojan logon, etc.

Incident rates are increasing alarmingly. The IMPACT associated with attacks continues to move up and off of the chart.

- Over 45% of the internal attacks resulted in losses over $200,000
- Over 15% of the internal attacks resulted in losses over $1,000,000
- Over 50% of the external attacks resulted in losses over $200,000
- Over 17% of the external attacks resulted in losses over $1,000,000

With so much threat and incident data available, creating an awareness of the problem and support for the solution should be a simple task. Hollywood has even pitched in by releasing a number of hacker-related movies. Who hasn't seen at least one of the following action thrillers: *Sneakers*, *Speed*, *Mission Impossible*, or *The Net*? Although these are highly dramatized, most of the underlying concepts are based on reality. So the awareness levels continue to increase. Why then, are we still so vulnerable? Why hasn't awareness translated into action? It's because organizations have a difficult time obligating funds to address problems they cannot physically see or touch. In Cyberspace, you can neither see nor touch (i.e., detect) a problem. All too commonly, it's way too late before you realize the damage is already done.

One incident highlighting the difficulty detecting and responding involved Citicorp. During the initial stages of the Citicorp attack, a group of cyber outlaws successfully transferred over $400,000 to off-shore accounts. The criminals were apprehended only after they chose to conduct a second attack. If they had called it quits after the first transfer, they may have never been discovered, let alone apprehended. As illustrated in Figure 2, a system or network looks the same (at least externally) from the time of initial reconnaissance through actual penetration and attack. If the network's risks are not adequately addressed, the only place you'll notice is the bottom line! When this is the case, you might not want to be the one to break the bad news to the Board of Directors and your shareholders.

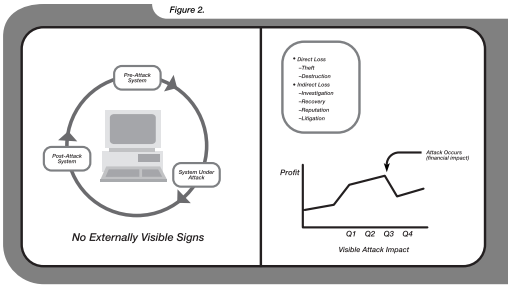

Figure 2. There Are Usually No Visible Signs of Attack – At Least Initially

Over the past few years a large number of commercial and government organizations have studied the challenges associated with reducing risk within such a complex environment. The U.S. Air Force and U.K. Defense Research Agency point out that on top of the aforementioned conditions, those tasked with defending the systems are now presented an operational risk environment with a greatly reduced decision and response cycle (see Figure 3). Typically, within the *Physical Domain*, decision makers have minutes, hours, days, or even weeks to respond to potential or actual attacks. This is not so in the world of Cyberspace. Within the *Virtual Domain*, the entire sequence associated with a network probe, intrusion, and compromise often can be measured in milliseconds or seconds. Also, an attacker need only locate one exposed vulnerability, whereas the system's defenders must address as many as 200-300 – all while supporting revenue-generating, or mission-enabling, operations. Therefore, the inner world of microchips and electrons is not an environment well supported by old-fashioned manual audits, random monitoring, and non-automated decision analysis and response. It is an environment requiring the sound insertion and placement of technical and procedural countermeasures as well as rapid, automated, responses to unacceptable threat and vulnerability conditions (attacks and misuse).

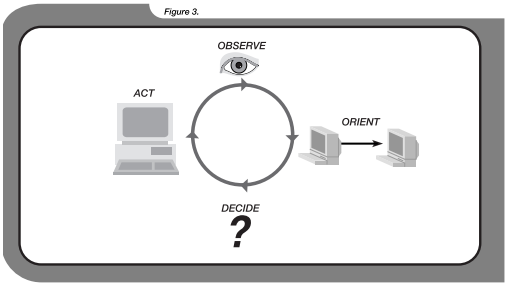

Figure 3. Automated Decision Support Is Required To Support The Needs Of The Virtual Domain

So what's needed? Are we fighting a truly stealthy opponent? Can we adequately secure and monitor our systems? We have a number of serious challenges, but solutions exist! We must first determine what is wrong. This will help us to substantiate the migration to the appropriate end-to-end solution.

The Wrong Approach

The primary challenges associated with bringing the network security domain under control deal primarily with its relatively new existence as a science and engineering discipline as well as the shortage of qualified professionals. Although some organizations have well-staffed and -trained network security staffs, this is not the norm. The norm is a small, highly motivated, yet out-gunned team that focuses most of its energies on user account maintenance, day-to-day fires, and general network design reviews. Few have time to study evolving threat, vulnerability, and safeguard (e.g., countermeasures) data, let alone develop policies and implementation plans based on the results. Even fewer have time to monitor actual network activity for signs of intrusion or system misuse. This has resulted in a ready-fire-aim syndrome and it does little more than create a drain on the organization. In military jargon it is referred to as "firing for effect." The following outlines the typical sequence of events within organizations implementing such an approach:

1. Organizational managers tend see the Network, but not in the context of the actual risk conditions. They understand the basic technology differences between operating systems such as Windows NT and Sun Solaris. They also understand how products such as Netscape, Internet Explorer, Word, Powerpoint, and Excel enhance their operations. But, they have little knowledge about the associated vulnerabilities that allow threats to enter, steal, destroy, or modify their most sensitive data.

2. As represented within Figure 4, safeguards are implemented in an ad hoc manner. This is largely due to an incomplete understanding of the problem. There is no real traceability to operational requirements, no study of the effects on threats or vulnerabilities, and no analysis of the return on investment. This approach can be summarized in the formula:
SECURITY = DIRECT TECHNICAL COUNTERMEASURES
(i.e., firewalls, encryption, security patches, etc.).

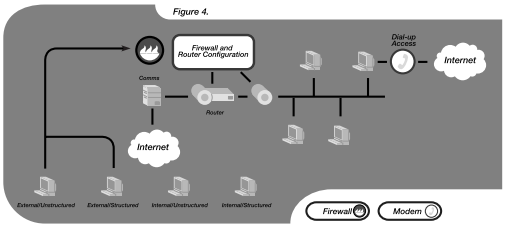

Figure 4. The Ad Hoc Approach To Safeguard Selection Does Not Work

3. As represented within Figure 5, organizations applying safeguards in this manner are left with a *false sense of security.* They believe they have addressed their risk, when in fact, many threats and vulnerabilities have not been taken into account. Considering the results of the various studies, it appears this approach provides an overall 20-30% solution.

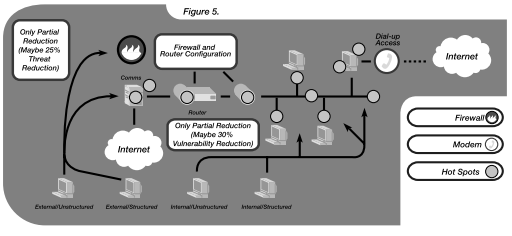

Figure 5. What The Network Really Looks Like

4. Over a relatively short period of time, the risk conditions further degrade. This network security degradation occurs as users alter system and safeguard configurations and work around safeguards.

To succeed in this environment is challenging and often impossible. This is especially true within a dynamic threat and vulnerability environment such as those within the typical Fortune 1000 company. The Security Program must provide comprehensive coverage of the threats, vulnerabilities, and assets, yet this approach only glances over the problem. As noted within Figure 6, network vulnerability conditions are complex and require much more than token attention.

The approach outlined within this section is obviously not the answer. Success within the virtual domain will depend upon the acceptance and adoption of sound processes that support a cyclic, adaptive security model. However, looking for management commitment for new processes, approaches, resources, and tools is much like asking your

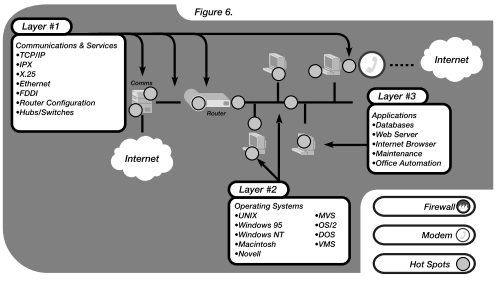

Figure 6. Vulnerabilities Are Located Throughout The Network Architecture

father for the keys to the family sports car. In this case, at least the facial expression and denial are similar. There are many specific variables associated with the network security problem domain. The ability to understand and present these variables to executive management in the context of how their organization will receive a return on investment is key.

A Good Start

The best place to start developing a new security solution is with that which is already understood and can be applied directly to the new problem domain. In this case, the best place to start is with the:

- Definition of sound processes
- Creation of meaningful and enforceable policies
- Proper implementation of organizational safeguards
- Establishment of appropriate program metrics and frequent program audits

Without established process and rigor, a successful reduction of network risk is highly unlikely. Constantly-evolving technology brings about a whole new set of problems not typically associated with the physical domain. Additional complexity is associated with the recent explosion of cooperative processing and data sharing. Our organizations struggle to understand the technologies and ever-evolving threats and vulnerabilities. All this and no rigor, process, or metrics leads to poor policy development and implementation. It also ensures a major variance (what many refer to as the GAP) between actual security program implementation and the organization's security policy. Without an understanding of the total risk to their networks and the many non-traditional variables associated with reducing such risks, these organizations quickly move to implement traditional baseline security solutions such as:

- Identification and Authentication (I&A)
- Encryption
- Access Control

This approach is known as Direct Risk Mitigation. Those implementing this approach will experience some reduction in risks but leave significant others unaddressed. The network security domain is too complex for such an ad hoc approach. Figure 7 provides a graphical representation of the perceived vs. actual risk reduction associated with the implementation of point technical solutions.

Figure 7.

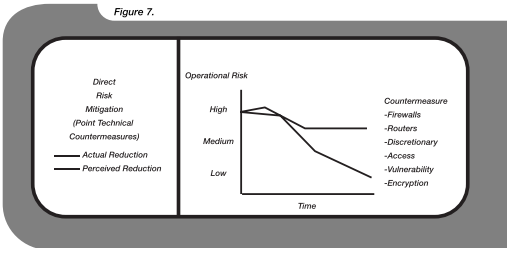

Figure 7. A One-Dimensional Security Program Provides Little Real Return

Although there are some major issues associated with transitioning physical security models and processes into the virtual domain, if adapted properly there are some significant benefits as well. This includes adapting some of the approaches to risk analysis, policy development, and traditional audits. Incorporating these basic components will provide the initial structure required to address many of the issues associated with the virtual domain. At a minimum, the Security Program must consist of well-trained personnel who:

- Adhere to sound standardized processes
- Implement valid procedural and technical solutions
- Provide for system audits intended to support potential attack or system misuse analysis

This approach is captured within the following formula:

SECURITY = RISK ANALYSIS
+ POLICY
+ DIRECT TECHNICAL COUNTERMEASURES
+ AUDIT

If implemented properly, this approach provides 40-60% of the overall security solution. Figure 8 is a graphical depiction of a very sound risk management model. This model begins with, as should all security programs, a risk assessment. The risk assessment is a policy support process. The risk assessment is the basis for the entire security program. The results of a risk assessment support operations and business planning efforts. Without proper risk analysis processes in place, the security policy and program lacks focus and traceability. Figure 9 provides a graphical depiction of the purpose and use of risk analysis. Once through the risk assessment portion of the cycle, those personnel responsible for implementation will acquire, configure, and operate the defined network solution. Until now, little had been done to ensure that clear technical policies were provided to these personnel. The lack of clear guidance and rationale resulted in the acquisition of non-value-added technical safeguards and the improper and insecure configuration of the systems once they arrived within the operational environment.

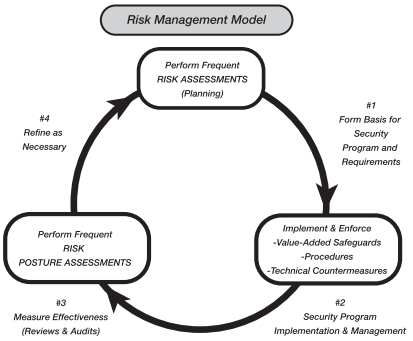

Figure 8. Implementation Of A Sound Risk Management Process Will Ensure Reduced Risk

One other major problem typically occurs within the implementation phase. Over time, administrators and users alter system configurations. These alterations re-open many of the vulnerabilities associated with the network's communications services, operating systems, and applications. This degradation has driven the requirement represented within the final phase of the risk management cycle – Risk Posture Assessments (i.e., audits). Risk Posture Assessments are linked, as all security activity should be, to the Risk Assessment results. Specifically, Risk Posture Assessments determine the organizational compliance levels, or variance, as related to the organizational security policy. The results of such assessments highlight program weaknesses and support continuous process improvement goals.

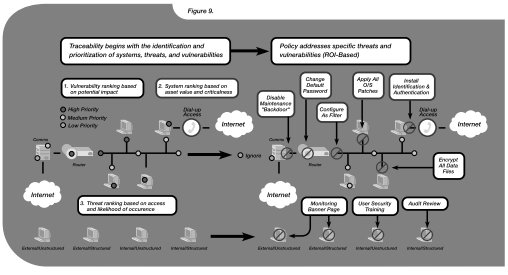

Figure 9. A Sound Risk Assessment Process Ensures A Sound Security Policy

The results of a Risk Posture Assessment are provided to a number of personnel in a number of formats (see Figure 10 for an example). They are provided to:

- Technicians and engineers in a format that supports corrective action
- Security/Network Managers in a format that supports program analysis and improvement
- Operations Managers/Executives in a format that summarizes the overall effectiveness of the security program and its value to the organization

The aforementioned approach is sound. It is also fairly responsive and simple to implement. That is, if organizations mandate the use of such processes organization-wide and use the tools available to support such tasks. But major problems still exist, and in total it only addresses 40-60% of the solution. These remaining issues cannot be ignored. The hackers do not care about the 40-60% covered; they only care about the 40-60% not addressed. Any success associated with this type of process depends upon proper initial system and countermeasure implementation and a fairly static threat and vulnerability environment. This is not the case in most organizations. Here's the 40-60% not addressed by this approach:

- An active, highly knowledgeable, evolving threat
- The greatly reduced network security decision and response cycle
- Network Administrators and Users misconfigure or working around countermeasures
- Low user awareness levels
- Highly dynamic vulnerability conditions

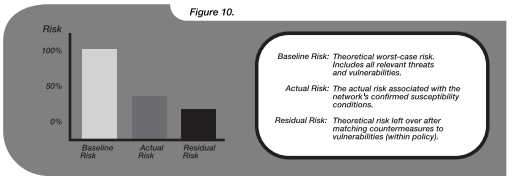

Figure 10. There Are Three Primary Risk Measurements

Although this is a good start, serious threats and vulnerability conditions still leave the network highly susceptible to attack and misuse. ISS and other leading network security organizations recognize these shortcomings and have developed the processes, technical framework, and initial toolset that address the environment's requirements for responsive, extensive, ongoing threat, vulnerability, and configuration analysis as well as increased user awareness. This solution is presented in the next section of this document. Introducing… the *Adaptive Security Model.*

The Right Answer - Adaptive Network Security

Adaptation is defined by Webster's Dictionary *as "The act or process of adapting. Adjustment to environmental conditions."*

This simple definition represents the missing link in most network security programs and it is also the most critical. It is not the initial selection, or implementation, of a security program that ensures day-to-day and minute-to-minute risk reduction. The processes and safeguard selection methodology (ROI-based) provides essential rigor, traceability, and documentation. Initial implementation puts the required structure in place. But the world of Cyberspace requires an adaptive, highly responsive process and product set to ensure ongoing, consistent risk reduction. This solution, and the Adaptive Security Model, is captured within the formula:

SECURITY = RISK ANALYSIS
+ POLICY
+ IMPLEMENTATION
+ THREAT/VULNERABILITY MONITORING
+ THREAT/VULNERABILITY RESPONSE

This approach is similar to the one adopted by most network management professionals for addressing performance risk issues. These professionals face very similar challenges and understand the importance of risk analysis, policy, and sound, consistent implementation. The organizations implementing such models are typically those with a large collection of highly complex networks. This collection of high-speed, high-performance components is supported by a variety of network management applications. These applications are designed to monitor key network performance events and anomalies and support rapid response to performance risk conditions. With these systems, network administration personnel can support network-wide account and file management, assess and respond to performance conditions, and if so desired, correct selected weaknesses and shortfalls. These systems support the ability to adapt to key operational and environmental conditions. Similar systems are in use by our telecommunications companies to adapt to global communications conditions. These systems even provide automatic signal re-routing if problems are detected within the path of any given signal.

The requirement for automated network management has been clear, and widely accepted ever since organizations first felt the pains associated with implementing networks larger than twenty to thirty systems. As networks, and our dependence upon uninterrupted operations, grew, so did the need for central management and automated network management systems. Currently, organizations invest in these systems with little or no hesitation, but it has been noticeably absent from network security management…until now!

Organizations such as British Teleco/Syntegra, Air Force Information Warfare Center, DISA, and DRA (UK) have studied the systems engineering and management approaches in relation to the network security environment. As a result, the personnel within these organizations have greatly contributed to founding the necessary framework for global network security standards, processes, and toolkits. ISS has further improved upon these approaches and defined the Adaptive Security Model. This model consist of the addition of a proactive, cyclic risk management approach that includes active network and systems monitoring, detection, and response. ISS has also developed, and is the only provider of, the technology toolset required to support all three variables as they relate to network threats and vulnerabilities. ISS' SAFEsuite® security product line works in concert with direct mitigation countermeasures and other monitoring tools such as anti-viral products. The SAFEsuite product line works much like traditional network management modules in that they support network monitoring, analysis, and automated response functions. The primary difference is based upon what is monitored and analyzed, and how the system responds. As depicted within Figure 11, a Network Security Management System is a natural outgrowth of the networked environment and provides overlapping, yet complementary network management services. Performance and Security Management systems are both required to support an organization's overall operational requirements.

The Operations Network Management Applications support traditional operations and performance variables, whereas the Network Security Management System will support the unique variables associated with the network security domain. Specifically, its architectural components will address and support the following:

Attack Analysis and Response:
Attack analysis and response is the real-time monitoring intrusion detection of attack recognition signatures and other suspicious activities including viruses, probing activity, and unauthorized modification of system access control mechanisms. Intrusion detection provides the ability to rapidly detect unauthorized hacker activity and respond with a variety of counter-threat techniques. Responses range from simple Security Officer notification to dynamic reconfiguration of identified weaknesses or communications paths.

Misuse Analysis and Response:

Misuse analysis and response is the real-time monitoring of internal misuse of network resources. Misuse is typically associated with activities not impacting operational effectiveness, but nevertheless counter to documented policy regarding acceptable use of organizational systems and resources (e.g., use of a corporate system for viewing pornography). Automated actions include denial of access, warning messages, e-mail messages to appropriate managers, etc.

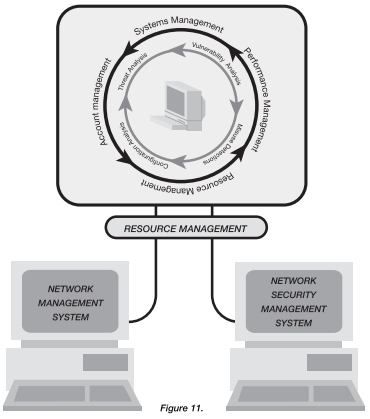

Figure 11.

Figure 11. Network Security Management System Components Complement Existing Technology

Vulnerability Analysis and Response:

Vulnerability analysis and response consist of frequent, automated, scanning of network components for unacceptable (by policy) security-related vulnerability conditions. This includes automated detection of relevant design and administration vulnerabilities. Detection of vulnerabilities leads to a number of user-defined responses including: auto-correction, tasking e-mails (corrective actions), and warning notices.

Configuration Analysis and Response:

This analysis includes frequent, automated scanning of performance oriented configuration variables.

Risk Posture Analysis and Response:

Includes automated analysis of threat activity and vulnerability conditions. This activity goes beyond basic (i.e., hard-coded) detection and response capabilities. It requires, and bases its response on, analysis of a number of variables such as asset value, threat profile, vulnerability conditions, etc. Analysis supports real-time technical modifications and countermeasures (e.g., denial of access, decoys, mazing, etc.) in response to dynamic risk conditions.

Audit and Trends Analysis:

Audit and trends analysis includes the automated analysis of threat, vulnerability, response, and awareness trends. The output of such analysis includes historical trends data associated with the Security Program's four primary metrics: (1) Risk, (2) Risk Posture, (3) Response, and (4) Awareness. This data supports program planning and resources decisions.

Real-Time User Awareness Support:

Provides recurring policy, risk, and configuration training. Ensures users are aware of key organizational policies, risk conditions, and violations of policy.

The *Adaptive Security Model* and related technology components listed above support organizational requirements to continuously ensure countermeasures are properly installed and configured. In this model, threats are monitored and responded to in a highly effective and timely manner and vulnerability conditions are analyzed and corrected prior to exploitation. It also supports the elimination of system misuse and increases general user and administrator security awareness. Figure 12 provides a graphical depiction of the *Adaptive Security Model* in place and its value to the overall security program. With the incorporation of the *Adaptive Security Model* and its support technologies, the entire spectrum of network security is addressed and measured. Internet Security System's SAFEsuite® of scanner and intrusion detection products have been designed to support all major aspects of this model. Although reaching 0% Risk is an impossibility, incorporating *Adaptive Security* processes and mechanisms supports reaching and maintaining the 100% solution – the best solution for any one specific organization.

In addition to appropriately and consistently addressing these unique network security variables, the technology modules support the requirement for defining, collecting, analyzing, and improving the Security Program's Operational Metrics. Figure 12 provides high-level examples of the types of program metrics required to support the reduction of risk and the NORMALIZATION of the network security problem domain.

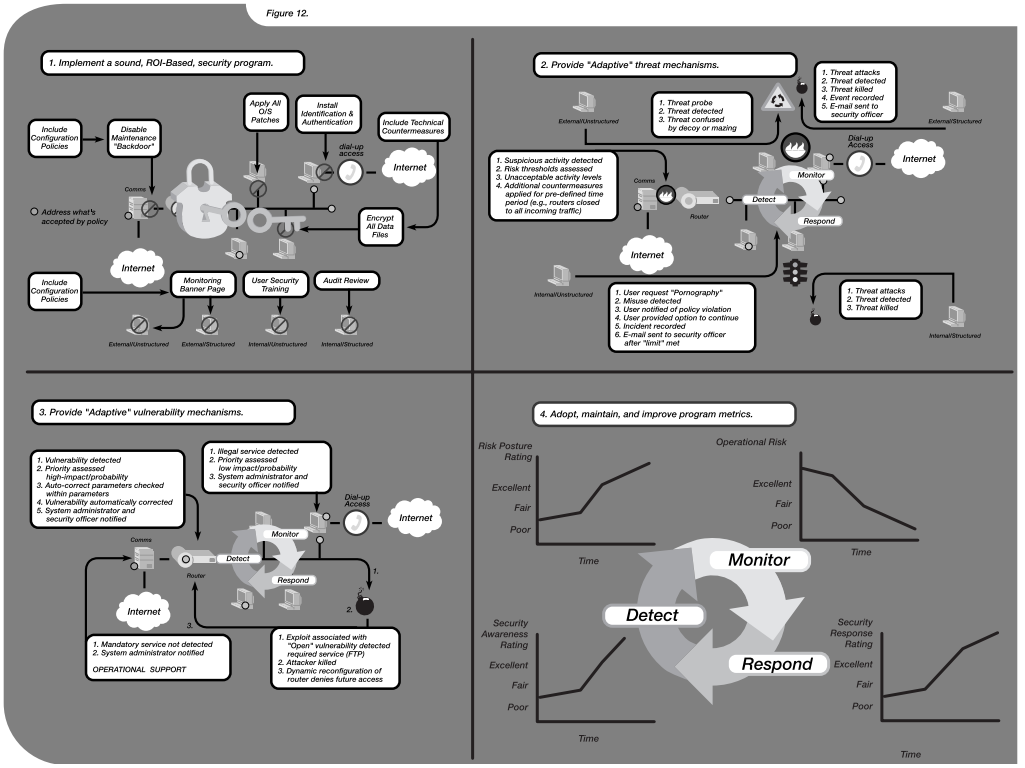

Figure 12. Implementation Of The Right Solution Is The 100% Solution

Summary

The network security domain holds many challenges in store for those entering the network and system security fields. We have not heard the worst of it. On the contrary, those on the offensive are just getting to know their environment and what they can and cannot get away with. The systems are too accessible and the payoff too big to stop! The structured threat continues to increase in size. Our networks continue to expand in size and complexity with little regard to the consequences. As well, organizational losses of $500,000 and more seem to attract little attention. This will serve only to encourage lawlessness and aggression. Organized crime, foreign intelligence organizations, and terrorist groups alike know of the power at their fingertips. It's not fantasy anymore – it's real! It was telling that of all those completing the WarRoom survey, no respondents answered one particular question. The question asked about losses associated with Electronic Funds Transfer. The lack of response is more telling than an actual answer.

So now we are aware of the problem and that a current answer of just throwing traditional technical countermeasures is not the solution. Industry and government organizations must quickly work to standardize rigorous, scientifically-based policy development, implementation, and monitoring standards and processes. It is not enough to change one organization. The networks are linked and the weakest link must be equally addressed.

The basis for today's organizational Security Program must evolve from the ad hoc approach to an analytical approach that includes sound analysis of operational requirements and accurate threat and vulnerability data. Technical countermeasures must be chosen based on their overall value-added and associated risk mitigation. These technical countermeasures must be accurately placed, configured, and maintained. Once in place, these direct countermeasures must be supported by an ADAPTIVE SECURITY MODEL (continuous threat and vulnerability monitoring and response) and applicable support products. These are the keys to significant and consistent risk mitigation.

No other process or technology can, or will, support the following security requirements:

- Ensure all applicable vulnerabilities are secured across the entire network
- Ensure all systems are configured in a secure manner consistent with organizational policy
- Ensure all potentially hostile threats are detected, monitored, and responded to in a timely, appropriate manner
- Provide real-time, on-the-fly, technical reconfiguration of threat access routes
- Provide timely security alerts and tasking to those responsible for addressing network threats and vulnerabilities
- Provide accurate network security audit and trends analysis data in support of security program planning and assessment efforts

If these issues are not adequately addressed, the entire security program may only provide cosmetic effectiveness, not an overall solution.

The solution is this:

SECURITY = RISK ANALYSIS
+ POLICY
+ IMPLEMENTATION
+ THREAT/VULNERABILITY MONITORING
+ THREAT/VULNERABILITY RESPONSE

Annex A: Glossary/Definitions

Attack Analysis and Response: Real-time monitoring of attack recognition signatures and other suspicious activities (including viruses, probing activity, and unauthorized modification of system access control mechanisms). Provides the ability to rapidly detect unauthorized hacker activity and respond with a variety of counter-threat techniques. Responses range from simple Security Officer notification to direct technical roadblocks.

Audit: Actions taken by a security or systems support staff to assess the differences between defined policy and actual implementation. These teams will address overall variance from policy, program trends, emergency or required corrective actions, and the organization's perceived ability to support the policies.

Audit and Trends Analysis: Automated analysis of threat, vulnerability, response, and awareness trends. Displays historical trends data associated with the Security Program's four primary metrics: (1) Risk, (2) Risk Posture, (3) Response, and (4) Awareness. Supports program planning and resources decisions.

Awareness Rating: Awareness applies to two primary measurements:

- User awareness of policies and procedures
- Network and Security Manager awareness of threat and vulnerability conditions

Configuration Analysis and Response: Frequent, automated scanning of systems configuration variables.

Incident: The actualization of a threat exploiting a vulnerability.

Misuse Analysis and Response: Real-time monitoring of internal misuse of network resources. Typically associated with activities not impacting operational effectiveness, but nevertheless counter to documented policy regarding acceptable use of organizational systems and resources (e.g., use of a corporate system for viewing pornography). Automated actions include denial of service, warning messages, e-mail messages to appropriate managers, etc.

Players: Other than the aforementioned threats, a number of personnel are associated with the network security problem domain. These individuals can be grouped into six primary categories. In order to optimize the overall security efforts, it is important to understand and address each of these according to its own unique attributes.

These groups are:

1. Accreditation and Certification Authorities: Those personnel assigned the responsibility of assuming the risk associated with a network by virtue of their review, testing, and approval of the network's security design and operational implementation. These personnel also need highly accurate data concerning the operational requirements, assets, threats, vulnerabilities, and safeguards. They must also periodically assess the security program metrics to ensure continued success of the security program.

2. Auditors: Those personnel assigned the responsibility of verifying the proper, consistent, and ongoing implementation of the security policies (both technical and procedural), analyzing its effectiveness, reporting security relevant trends, and monitoring possible illegal or inappropriate activity.

3. Executive Decision Makers: Those personnel typically responsible for the overall success and fulfillment of the organization's operational goals, risk management program, budget management, and technical direction. These personnel typically need to understand the security program from a return on investment perspective. They need to understand their specific threat and vulnerability conditions as well as the value of individual safeguards and the overall security program.

4. Implementation Personnel: Those personnel assigned the responsibility of implementing the security policies and procedures (including technical implementation). These personnel include system security officers, system administrators, network engineers, users, etc.

5. Network/System Users: Those personnel (typically operations personnel) using the system to fulfill their operational tasking.

6. Policy Makers: Those personnel tasked with assessing operational and security variables in order to develop and enhance organizational technical and procedural policy documents. These personnel need accurate data concerning operational assets, threats, vulnerabilities, safeguards/countermeasures, and security program metrics.

Policy: Formal and enforceable organizational requirements for the configuration, implementation, and operation of network or security systems. These requirements are preferably based on a formal operational risk assessment that takes into consideration operational network requirements (capabilities, performance, and cost), threat and vulnerability conditions, etc.

Real-Time User Awareness Support: Automated user awareness support. Provides recurring policy, risk, and configuration training. Ensures users are aware of key organizational policies, risk conditions, and violations of policy.

Residual Risk: Risk remaining after an organization applies (as defined within organizational policies) safeguards to various threats or vulnerabilities. For example, an organization may choose to allow FTP or NFS services. The risk associated with these vulnerabilities is accepted and considered residual risk.

Response Rating: Response applies to two primary measurements:

- The amount of time associated with threat and misuse detection and response.
- The amount of time associated with vulnerability or configuration detection and response

Risk: The likelihood of loss or damage based on threat, vulnerability, and consequence analysis and the likelihood of an incident.

Risk Posture Analysis and Response: Automated analysis of threat activity and vulnerability conditions. Automated Decision Support (ADS). Analysis supports real-time technical modifications and countermeasures (e.g., denial of access, decoys, mazing, etc.), in response to risk conditions.

Risk Posture Rating: Included within the Risk Posture Category are a variety of measurements. Measurements include:

- Policy vs. Actual Compliance Levels
- Vulnerability Trends Analysis
- Threat Trends Analysis
- Activity Analysis

Risk Rating: Organizations typically desire a low-risk operations and network environment. Understanding the differences between high and low requires an understanding of the network's assets, threats, vulnerabilities, and safeguard/countermeasure conditions. These factors must be quantified in order to understand the impact of various safeguards and countermeasures.

Safeguards/Countermeasures: Those actions taken to either eliminate or reduce the risk associated with a threat or vulnerability. Examples include firewalls, patches, discretionary access control, configuration guidance, etc. ISS refers to safeguards as corrective actions.

Security Program: The security program is the documented organizational approach to reducing and managing those operational risks associated with human threats. It includes people, policies, processes, and technical countermeasures and support aids.

The Security Program must fulfill three primary requirements:

1. Support all operational requirements
2. Address all relevant threats and vulnerabilities
3. Respond to the needs of planners, implementers, accreditation/certification personnel, auditors, and managers

Technology Environment: All too often the systems support staff has little understanding of the technical risk conditions associated with their networks. This is perfectly natural considering today's high-tempo operational environments, but it needs to be addressed. A solid understanding of the primary technology is essential to understanding the network security problem domain. Currently, the lack of network security expertise is a major contributor to the high-risk environment within which our networks operate. We have an extremely high technology turnover rate, a drive for more and more cooperative processing, shared resources, Internet and intranet connectivity, and highly vulnerable operating systems, network protocols, and shared applications. In addition, IT literacy rates continue to increase while network security literacy levels show only gradual increases. The network security technology environment is currently characterized by a number of disjointed point security solutions. These technologies primarily focus on one particular aspect of the network security problem set, yet are marketed as total solutions. Although many of these solutions offer excellent risk reduction gains, they provide little return if not implemented properly and complemented by overlapping processes and technology. The threats associated with the network security domain have little regard for what IS protected and tend to target that which IS NOT protected.

Threat Assessment: A Threat Assessment includes those actions taken by a team of highly skilled operational and threat analysts to assess human and environmental threat activity in relationship to a specific organization or geographic area. Their primary intent is to establish a likelihood or probability of occurrence for specific threat categories. This data supports an eventual risk assessment (analysis of threats, vulnerabilities, and organization assets).

Threats to the Operations and Assets: Security professionals worldwide face an interesting challenge when asked about the threat to information systems. On one hand, they are armed with file drawers full of threat statistics and incident data. On the other hand, they do not have the dramatic physical proof of destruction such as broken windows, doors, and safes. The evidence consists of boring bits and bytes or painfully long and technical audit trails. None of which support the creation of a compelling or emotional argument. They can choose to quote the FBI, CSI, Government Accounting Office, the Big Six Accounting Firms, and a large number of other sources. The availability of threat data is no longer the

problem. It is conveying this data in a manner that portrays an accurate picture without coming off as a self-interested alarmist. It is also in providing the data in terms relevant to the ultimate solution (i.e., the right data, in the right format, at the right time). Discussions of successful hacks or attacks provide little value without appropriate details related to the specific threat and vulnerabilities exploited. The current threat environment is alarming. The average Internet user can access over fifty hacker tutorials and Web pages in less than ten minutes. From these sites they can build a library of network exploitations or download hacker tools that provide even common users the ability to probe (i.e., automated vulnerability scan) and attack complex networks. The number of hostile threats continues to increase, as do incident and organizational impact levels. The threats now outgun the defenders and will continue to do so until innovative risk management techniques are standardized and implemented. Categorizing threats allows security professionals to apply safeguards in a traceable manner. The number of categories is not as important as the ability to link these categories to corresponding vulnerabilities and eventual safeguards. ISS' four basic categories of human threat include:

1. Internal/Unstructured: The average system user. Lacks real awareness of technical vulnerabilities. Typically responsible for device errors and network crashes through inadvertent misuse and poor training. When this category exploits network systems for illegal gain they typically misuse authorized privileges or exploit obvious errors in file access controls.

2. Internal/Structured: The deadliest threat – an authorized user with advanced knowledge of the network and its vulnerabilities. These threats typically make use of their physical and electronic access to resources and assets. Using tools and special techniques, this class of threat can easily work around simplistically configured networks, even if a sound security policy exists. A much more proactive security program (augmented by aggressive network system and file misuse and intrusion detection systems) must be in place to significantly reduce this threat.

3. External/Unstructured: The average curious Web surfer. This class of threat includes those individuals with access to basic scanning tools and simplistic hacking exploits but without the requisite skills and motivation to either perform the actual exploitation or gain deep (root) access. Their activity typically leads to inadvertent system crashes and lost data files.

4. External/Structured: The most feared and increasing threat. This threat typically has detailed knowledge of your network's vulnerabilities and access to available and tailored hacker tools. This class of threat generally can work around most organizational security programs. That is to say, if they believe that the target systems are not configured in a manner that places the attacker at risk (of detection and apprehension). They take advantage of not only technical vulnerabilities, but gain access to sensitive data through dumpster diving, personal interviews and persuasion, publicly available resources, etc.

Understanding Operations and Assets: Operations are those organizational activities associated with fulfilling mission requirements. They are the activities typically associated with bringing in the money. Examples include manufacturing, research, sales, etc. Associated with these operations are organizational assets. Assets can be any of the following: monetary, material, resource, or information. Assets are generally those items, which if lost, would significantly impact an organization. Inadequate understanding of operations and assets typically result in:

- Costly (financial and risk-related) safeguard investment decisions
- Inappropriate safeguard selection
- Misplacement of safeguards
- Fatal credibility loss for those representing the security program and/or budget

Vulnerabilities: Widespread availability of technical vulnerability data is, and should be, of great concern to those relying upon automated systems. Vulnerability data is available from a number of sources. In most cases, individuals desiring such data can also gain access to automated tools that make scanning your network for weaknesses as simple as pushing the Return key. Of course these same, and better, tools are also commercially available for those responsible for securing organizational networks. They allow network security professionals to monitor and assess their organizational vulnerability conditions in relation to relevant policies. The vulnerabilities associated with networks are not magic. Both sides (the good guys and the bad guys) understand what and where they are. They can be exploited or mitigated depending on the person's role. Vulnerabilities, like threats, must also be categorized in order to ensure adequate analysis and support eventual application of safeguards. As noted in Figure 6, the vulnerability categories apply to: (1) Network Communications and Services, (2) Operating Systems, and (3) Applications. Addressing each is necessary to developing a sound security program. The three general categories of vulnerabilities include:

1. Design: Those vulnerabilities actually designed into the system. Examples include various UNIX and network services (e.g., FTP, TFTP, and Finger), Ethernet, X.25, allowing weak passwords, HTTP, Windows reg file association, X Window Session, etc.

2. Implementation: Those vulnerabilities created or allowed due to operational requirements (e.g., allowing FTP without a security patch for operational support reasons.)

3. Administration: User and Administrator misconfiguration vulnerabilities. Improperly addressing those vulnerabilities addressed by policy and supported by technology (e.g., discretionary access control). For example, improper setting of file access controls and user privileges, selection of weak passwords, etc.

Vulnerability Analysis and Response: Frequent, automated, scanning of network resources for unacceptable security-related vulnerability conditions. Automated detection of relevant design and administration vulnerabilities. Detection leads to a number of user-defined responses including auto-correction, tasking e-mails (corrective actions), and warning notices.

Vulnerability Assessment: Actions taken by a team of highly skilled technical and procedural vulnerability analysts to assess an organization's overall vulnerability conditions. Optimally, these teams define all possible vulnerabilities, then focus on the most likely to occur within the assessed organization. They will then conduct tool-assisted or manual analysis of the organization's most significant risk (threat and vulnerability pairings) and provide final reports that include risk conditions, safeguard recommendations, and policy guidance.

Annex B: Acknowledgements

Authors:

Jeffrey Z. Johnson: Mr. Johnson is the National Director of Strategy and Operational Services. He has over 15 years of experience within the various technical security and consultancy fields. He has designed, implemented and managed a number of highly complex, secure, worldwide networks. He was also the lead or co-lead for a number of popular Information Warfare and Risk Analysis efforts. Mr. Johnson was the Lead Inventor of Trident Data System's network risk assessment application, NetRISK, and is now responsible for leading ISS' Scanner and Automated Decision Support efforts. He is a graduate of The University of New York, Albany.

Chris Klaus: Mr. Klaus is the Founder and Chief Technical Officer of Internet Security Systems (ISS). He has a great deal of experience within the technical vulnerability and analysis fields. He provides organizational risk consultancy support to many key Government and Fortune 500 companies and is an internationally recognized network security expert. He also provides technical direction and leadership to each of ISS' product teams, including ISS' Internet Scanner, System Security Scanner (S3), and RealSecure. He attended Georgia Tech.

Patrick Taylor: Mr. Taylor is the Director of Strategic Marketing for Internet Security Systems (ISS). He has managed all aspects of strategic product marketing development efforts. He has an in-depth understanding of network threat and vulnerability conditions and has supported a large number of commercial and government vulnerability assessments. He is directly responsible for leading the planning efforts for an integrated network security management system (SAFEsuite®). He is a graduate of Georgia Tech and received his MBA from Harvard.

Contributors (Direct and Indirect)

The following personnel contributed to the approaches and overall content of this paper through either formal submissions, review, and/or past discussions. Their input is greatly appreciated and ISS thanks all of them for their support and contribution. The presence of the non-ISS names does not reflect formal support of the views or approaches contained within this document.

Keith Cooley (Vice-President, ISS)
Mike Corcoran (DRA)
Tim Dodd (Sr. Applications Developer, ISS)
Karen Freeman Worstell (Network Security Consultant)
David Gerulski (Product Manager, ISS)
Nick Hiscock (DRA)
David LeBlanc (Sr. X-Force Engineer, ISS)
Derek Long (Sr. Consultant, Syntegra)
Craig Robinson (President, Commercial Operations)
Tamara Savino (Technical Documentation Manager, ISS)
Mike Warfield (Engineering Manager, ISS)
Mark Wood (Product Manager, ISS)