Compliance, Part II:

Risk Abatement, Strengthening Justification and Documenting the Security Process

Copyright© 2006 Internet Security Systems, Inc. All rights reserved worldwide

INTERNET|SECURITY|SYSTEMS®
Ahead of the threat.™

Table of Contents

RISK MANAGEMENT AND ABATEMENT

Government regulation encourages companies to take a top-down assessment of the information security risks to their enterprise. Once risks are identified, the companies inevitably question how they can best protect against those risks. ISO 17799 provides some guidance by indicating that protection strategy starts with risk assessment and ends with a set of security requirements.

"Security requirements are identified by a methodical assessment of security risks.[1]"

How does ISO 17799 define risk?

"Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.[2]"

Though not a strict definition of risk, ISO 17799 ties an ambiguous term, risk, to the more concrete terms of assets, vulnerabilities and threats. With the proper tools, one can identify or clarify assets, assess where those assets are vulnerable and associate threats with the vulnerabilities they seek to exploit.

THE RISK EQUATION

The risk definition above can be written as an equation, which lends further insight into how risk can be reduced. Though this equation takes on many different forms, the core risk equation follows:

*Risk = Assets * Vulnerabilities * Threats*

The equation more directly indicates that risk increases as a function of rising numbers of assets, rising numbers of vulnerabilities and/or rising numbers of threats. Therefore, reducing the number of assets, reducing the number of vulnerabilities and/or reducing the number of threats can reduce risk.

Though it may be conducive to risk abatement, reducing the number of assets clearly is not conducive to good business since businesses aim to grow their assets, not reduce them. Furthermore, the Sarbanes-Oxley Act was instituted to rebuild investor confidence in published financial statements to encourage investment. If businesses were to sell off assets for the sole purpose of reducing risk, this would actually discourage investment.

Reducing the number of threats is not feasible if businesses rely solely on legacy security systems (such as antivirus and firewalls) that block established threats but do not recognize new, "zero-day" threats. Reactive security technology does not reduce risk levels. **The primary point of risk abatement is to select controls that reduce risk well in advance of a successful attack (proactive protection), not to implement threat countermeasures after impact (reactive protection)**.

Security companies offering pattern-match signature technology fall into the reactive countermeasure category. **Threat countermeasures do nothing to proactively address and resolve the original vulnerability; they can only react to individual threats**. Because threat countermeasure companies do not understand software vulnerabilities, their only option is to wait until the threat reveals itself (does damage) and becomes widespread enough (reaches critical mass) before developing an actual threat countermeasure for that one threat. Clearly, threat countermeasures are reactive and can only be implemented after the threat has already caused unwanted harm.

Critical to understanding the distinction between threat countermeasures and vulnerability protection is the fact that even though threat countermeasures may be in place, the vulnerability still exists, unaddressed and unresolved. Why is this so critical? Because threat countermeasures *do not enable* significant strides in true risk abatement. In fact, as we will see, threat countermeasure companies actually introduce undesirable risk into the enterprise because they are focused on threats as opposed to vulnerabilities. The next threat that targets that same vulnerability *will* succeed because there is no pattern-match signature for this new threat. There is no threat countermeasure for this new threat. **Pattern-match security companies are doing nothing to address the vulnerability, but instead only develop signatures, or threat countermeasures, on a reactive exploit-by-exploit basis**.

So where does this leave companies seeking to lower the risk of attack? It is impractical to reduce the number of assets. Dealing with threats is reactive and does not truly abate risk. The only variable left in the risk equation is the vulnerabilities. Reducing the number of vulnerabilities affords companies with some measure of control over risk. Threats require some sort of vulnerability in order to inflict damage to the enterprise. **Take away the vulnerability and the threat loses its power to inflict damage**. The following compliance scenario illustrates this concept much more clearly.

THE CHECK-SIGNING PROCESS CONTROL

This example explores a company's check-signing process control and its impact on risk. Currently, this process control requires only one authorized person's signature to sign checks for large sums of money. Consider each variable in the risk equation.

What is the inherent risk with this current process control? The risk is the probability that a dishonest employee could steal large sums of money by having the power to sign corporate checks without having to secure another corporate signature.

What is the **asset at risk** in this scenario? Large sums of money.

ISO 17799 defines vulnerability as follows:

"[V]ulnerability – a weakness of an asset or group of assets that can be exploited by one or more threats.[3]"

What **vulnerability** is present in this check-signing process control? Absence of accountability.

ISO 17799 defines a threat as follows:

"[T]hreat – a potential cause of an unwanted incident, which may result in harm to a system or organization.[4]"

What is the **threat** in this example? The dishonest employee that would steal large sums of money.

How could effective risk management abate this risk? A top-down risk-based assessment would recognize that the current check-signing process control is indeed risky and should be strengthened to abate risk. Changing this check-signing process so that two people are required to sign checks for large sums of money greatly reduces the risk to the organization.

How exactly was this risk abatement accomplished? Risk was abated by directly addressing and resolving the vulnerability. The absence of accountability (the vulnerability) was replaced by an appropriate level of accountability. Notice the threat, the dishonest employee, may still work for the corporation, but the mere existence of accountability greatly reduces the probability that this threat will ever be successful. Again, whether the threat would ever actually exploit this vulnerability is not the issue here. **The fact that a risk exists, however likely, demands a response to address that risk**. In this example, the check-signing process control was strengthened to properly abate risk. This is exactly what the Public Company Accounting and Oversight Board (PCAOB) meant when it stated:

*"Section 404 of the [Sarbanes-Oxley] Act aims to **strengthen the internal controls that underpin the accuracy and reliability** of a company's published financial information.[5]"*

By strengthening this check-signing process control, the company has further reduced the risk of fraud, thereby increasing investor confidence in subsequently published financial information.

Returning to the check signing example, how else could this risk have been addressed? Had the company suspected a dishonest employee with the authority to sign checks, it could have fired the employee before they had a chance to steal any money. But again, this would not have alleviated the original vulnerability (the faulty check-signing process) and a newly hired employee could just as easily take advantage of the policy to steal money.

This scenario highlights the importance of not only addressing and resolving enterprise vulnerabilities, but also of **allowing the risk assessment to drive the selection of controls. Remember, control selection in and of itself (without ties to risk abatement) is not sufficient and probably will not demonstrate compliance**.

ABATING NETWORK SECURITY RISK BY ADDRESSING SOFTWARE VULNERABILITIES

One can draw an analogy between the check-signing process control scenario above and network security. Through remediation and protection of software vulnerabilities, a security solution can reduce the risks associated with malicious code ("malcode"), unauthorized access, security breaches and other threats. However, **true risk abatement must occur by addressing the vulnerabilities resident within business assets rather than applying countermeasures to threats. In the check-signing example, the risk remained when the vulnerability was not addressed**.

So how do you get this type of vulnerability protection for your network? First of all,

"Something cannot be protected if it is not understood.[6]"

To protect vulnerabilities, they must first be understood. Only then can the security vendor leverage this understanding to implement protection. This understanding, or security intelligence, manifests itself in high-risk software vulnerability research and discovery. Questions to consider when evaluating security vendors include:

Which security vendors research high-risk software and system vulnerabilities inadvertently created by other companies?

Which security vendors are actually securing software and system vulnerabilities created by other companies? Is this not what network security companies should be doing?

Researching is not enough. The security vendor must also be able to translate this security intelligence into vulnerability protection embedded within its security products.

Security software itself must be free of vulnerabilities. If the security vendor's software and systems are prone to being exploited, how can they protect the customer? Hackers could exploit the security vendor's software, turn off the security vendor's protection and wreak havoc within the enterprise. Ironically, using certain security vendors' software to gain access to the enterprise is indeed happening.

*"Today, professional criminals have moved in and **targeted a critical weakness in many anti-virus programs**.[7]"*

*" … **[S]oftware programs designed to protect data have themselves become the targets** … These include **backup software, antivirus software**, database software and even media players. **Flaws in these programs** put critical national and corporate resources at risk and have the potential to compromise the entire network.[8]"*

*"Already, **hackers are bypassing or disabling Symantec software** in their efforts to access personal information or spread viruses and worms. And there's mounting evidence that hackers are trying to use **Symantec software as an actual gateway into corporate servers and PCs**.[9]"*

Not only must the security vendor provide vulnerability-based security content that protects ahead of the threat, it must also ensure that its software and systems are free from vulnerabilities. Otherwise, hackers will be able to leverage security software as a gateway into the enterprise.

BUYING CRITERIA

What should you look for in a security vendor in order to properly abate network security risks?

1) **Vulnerability research** into high-risk software vulnerabilities, whether the vulnerability is its own or another vendor's; the end goal is to protect the customer from high risk software vulnerabilities regardless of source.
2) **Vulnerability protection** that leverages primary vulnerability research to implement proactive risk-based vulnerability protection rather than reactive pattern-matching threat countermeasures for individual threats.
3) **Vulnerability-free software** and systems to ensure that the solution is not compounding the risk management and abatement problem — not introducing more risk into the network infrastructure.

For more information on software vulnerabilities and the difference between software vulnerabilities and the threats that exploit them, refer to the white paper, "Lifecycle of a Vulnerability," located at http://www.iss.net/support/documentation/whitepapers/index.html.[10]

STRENGTHENING JUSTIFICATION USING A MESH OF CONTROLS

In the "Guns, Guards and Dogs" illustration discussed in Part I of this white paper (http://www.iss.net/support/documentation/whitepapers/index.html), implementing a mesh, or complementary combination, of controls provides a greater level of security and peace of mind than can be achieved with just one control. This is because a defense-in-depth strategy provides broader security coverage. The mesh of controls strategy has been validated for compliance and supports a company's justification for control selection.

*"View controls collectively — using **a mesh of controls that support each other** can strengthen justification.[11]"*

This is true for physical controls such as guns, guards and dogs, as well as network security. Over-reliance on any one technical control not only limits the breadth of coverage but also provides opportunities for unwelcome exposure.

"The need to blend and combine multiple controls to achieve a meaningful degree of security is likely to never change.[12]"

A HOST-BASED MESH OF TECHNICAL SECURITY CONTROLS

One example of blending and combining multiple controls can be found in Host-based Intrusion Prevention Systems (HIPS). HIPS blend and combine different protection styles to provide multiple layers of protection for different types of code behavior. However, not all HIPS products are the same. Some HIPS products do not provide vulnerability protection and therefore do *not* meet the buying criteria that includes vulnerability research, vulnerability protection and vulnerability-free software and systems.

*"The explosion of current online threats could unseat traditional anti-virus technology and the companies that sell it from the front lines of computer defenses as **users turn to more proactive technologies**, experts say.[13]"*

This is not to say that pattern matching, or threat countermeasures, do not have a place in the HIPS arsenal of protection styles; but the role of threat countermeasures has changed.

*"Only pattern matching can reveal a virus' name, and we need to know that for two reasons. First, we have to **know the name to clean the virus off our systems**, and second, we need to **know what damage it might have done**."*

*"But when trying to detect zero-day virus attacks — those that exploit software vulnerabilities that software vendors have not yet discovered — **we need to catch the infections before the detection pattern arrives from the vendor**.[14]"*

The pattern-match security vendors identify and eventually block (given enough time to develop attack signatures) the "known bad," allowing all else. A firewall allows the "known good," blocking all else. However, protection is also necessary for a third level of knowledge about code: the unknown code. Hence the need for a **vulnerability protection vendor that prevents zero-day attacks, or unknown code**, from inflicting harm. Vulnerability-based protection is now shouldering an increasing share of security responsibility and can even protect vulnerabilities in antivirus and backup programs that might be used by hackers to gain access to the corporate network.

*" … **[S]oftware programs designed to protect data have themselves become the targets** … These include backup software, antivirus software, database software and even media players. **Flaws in these programs put critical national and corporate resources at risk** and have the potential to compromise the entire network.[15]"*

In addition to vulnerability protection, the ideal HIPS vendor would also provide Application Inspection in order to thwart malicious code before it starts executing on a machine. How does the code get past the vulnerability-facing network inspection? Perhaps this malicious code does not exploit any software vulnerabilities, but rather relies on social engineering, convincing a gullible user to kick off an executable code. By utilizing Application Inspection, the preferred HIPS vendor stops malicious code before it can execute.

In summary, Host-based IPS solutions with multi-layered protection technology are becoming part of the rising standard of due care. Interestingly, related research activities are also becoming part of this standard of due care as well.

"Endpoint security (agents): … Firewall-like capabilities must be blended with application integrity and control and host intrusion protection — at a minimum.[16]"

"If all servers in the processing system (not just the servers holding the data) were protected with effective HIPS, more than half of the reported compromises could have been prevented.[17]"

"The second item is the existence and comprehensiveness of related research activities by the product vendor. This is absolutely essential to maintaining and even improving effectiveness of the capability.[18]"

For more information about which HIPS vendors utilize which protection styles, refer to Gartner's article, "Understanding the Nine Protection Styles of Host-Based Intrusion Prevention.[19]"

MULTIPLE INTRUSION PREVENTION SYSTEM IDENTIFICATION AND ANALYSIS TECHNIQUES

Blending and combining multiple controls within an Intrusion Prevention System (IPS) protection engine is critical to accurate and comprehensive identification and analysis. This is true for both host- and network-based IPS. The first step to preventing intrusions is correctly identifying those intrusions to begin with. Using a combination of identification techniques and cross-checking each method against the others not only increases the accuracy of identification and analysis, but also removes the risk of security control evasion that may exist due to over-reliance on any one particular technique. Though today's IPS should utilize multiple identification techniques, some do not. Even now, several vendors over-rely on Port Assignment as an identification technique, which leaves their customers open to security control evasion on non-designated ports.

For more information on the different identification and analysis techniques, refer to the Internet Security Systems (ISS) white paper, "Defining the Rules of Preemptive Protection: The ISS Intrusion Prevention System.[20]"

SCAN AND BLOCK . . . PATCH MANAGEMENT ON YOUR SCHEDULE

Another useful mesh of technical security controls is the ability to scan for vulnerabilities without worrying about those same vulnerabilities being exploited. What layers are referred to here?

- Vulnerability protection provided by host- and network-based intrusion prevention
- Vulnerability scanning and remediation provided by vulnerability management

Furthermore, an added bonus to using vulnerability-protection security vendors is that enterprises are able to test and deploy patches on their schedule. When enterprises deploy vulnerability-based protection, they no longer race to patch systems before a potential attack. Instead, they can trust the vulnerability protection for security while conducting assessments and remediation on their own terms and schedule.

ENABLING ENDPOINT COMPLIANCE THROUGH A COMBINATION OF CONTROLS

In the case of determining whether to allow a remote user access to the company network, it is important to be sure that the remote desktop agent is updated to the correct version before granting the user access to corporate resources. Otherwise, he or she could potentially introduce malicious software onto the network. Working together, security management, network IPS and desktop agents run desktop version checks to determine whether to allow that mobile user onto the network. Without having such a unified mesh of different controls working together, companies are instead forced to hope that a particular user will not unknowingly infect the network. Auditors do not award compliance credit for "hope."

MULTI-FUNCTION SYSTEMS – COST-EFFECTIVE SECURITY SOLUTIONS

Recall that the preferred HIPS vendor provides multiple layers of comprehensive protection at the host level for three levels of knowledge about code: blocking the known bad (and allowing all else), allowing the known good (and blocking all else) and blocking unknown code. In the same way, multi-function security appliances provide comprehensive protection for these three levels of knowledge about code, but instead do so at the *gateway*. In addition to traditional security technologies such as firewall and antivirus, multi-function security systems also utilize intrusion prevention, Web filtering, content filtering and antispam technologies. Just as not all HIPS products are equal, the same is true for multi-function systems. The vulnerability-protection security vendors utilize vulnerability-facing network inspection and application inspection to provide defense-in-depth coverage for unknown code, whereas the threat countermeasure security vendors do not.

INTERNAL SECURITY

Thus far, we have addressed host, network and gateway protection, but what about the internal network? Should we not also be concerned about internal misuse and abuse? What about worm propagation that originates from within? How can we address threats that appear to start from inside the network?

"The proliferation of alternate paths into an organization, application-layer attacks, and devastating worms/malware are all hammering home the conclusion that ***perimeter defenses must be complemented by a full range of internal security measures. Addressing this need will inevitably require implementing a combination of different types of security controls****. However, taking advantage of products that are better tuned to the unique challenges of internal security will be instrumental to economically achieving an effective internal security solution.[21]"*

Internal segmentation and firewalls are several of these aforementioned controls. As a matter of fact, an internal firewall is a requirement for PCI [Payment Card Industry] compliance.

"Internal segmentation (e.g., using routers, switches, and virtual LAN technology) supports logically or physically separating resources that require different levels of security."

"Internal firewalling also facilitates segmentation, but does so with the added benefit of providing a more effective security barrier, where needed.[22]"

Network behavioral anomaly detection systems (NBADS) provide the network visibility required to both secure the internal network and conduct network planning. NBADS monitor for violations to acceptable use policies by providing a greater degree of visibility into host relationships than has been possible before. Furthermore, NBADS can lock down the internal network to allow only a whitelist of known, good relationships which enables 99 percent of legitimate network traffic to continue while blocking 100 percent of illegitimate traffic. Finally, by providing insight into host relationships, NBADS can help network teams plan how to best segment and firewall the internal network.

Internal security is slowly becoming part of the standard of due care which was discussed in Part I of this paper.

"A common component of many of these regulations is that impacted organizations must establish "comprehensive information security programs." Thus, while we expect regulators to focus on well-known "basics" during their first rounds of audits against associated requirements, ***we also expect their investigations to focus soon thereafter on protective measures being taken for internal networks and systems****.[23]"*

ENTERPRISE MESH OF SECURITY CONTROLS

HIPS, IPS, vulnerability management, multi-function systems and internal security each utilize a blend, or combination, of controls to provide broader security coverage for malicious code. Yet, when implemented together as an enterprise-wide security solution, they have the *potential* for producing an even more tightly interwoven series of meshes.

"Finally, the ability to integrate with the same management applications used for the perimeter environment would also be valuable.[24]"

To convert this potential into reality requires central and unified management of the entire mesh. Without centralized management, this mesh quickly becomes nothing but an unmanageable mess. As we examine central, unified management of this enterprise mesh of technical security controls, we will see how these technical security controls can be governed by security process controls embedded within the very same security management tool.

CENTRAL MANAGEMENT: DOCUMENTING THE SECURITY PROCESS WHILE ORCHESTRATING THE MESH

We have established that an enterprise mesh, or complementary combination, of technical security controls not only has *compliance potential* to provide strong justification before auditors, but is needed to provide a meaningful degree of security. Without central management for this combination of controls, this enterprise mesh simply becomes an unmanageable mess.

CENTRAL MANAGEMENT ENABLES THE MESH AND AVOIDS THE MESS

How can corporations unify and orchestrate independent controls with any consistency if each control requires its own management tool? When do these controls cease to be a complementary blend working together and instead become independent silos operating separately and distinctly? Also, how can any security professional make sense of the endless streams of security data without one place to automatically aggregate, correlate, prioritize and produce actionable steps for the network security team? Without this capability, who can make sense of it all without also compromising security? With different management tools, who compiles the results to provide a complete view of the enterprise risk level?

With no central management, not only do the communications, reporting and auditing become unmanageable; so do deployment, management, configuration and data analysis for the large numbers of appliances, agents and applications under management. Consistent security policy application and product and content updates must be considered as well. Employing a security information and event management tool may address a small piece of this central management problem but clearly does not address all the central management issues. Central management demands a two-way dialogue between the manager and the technical controls. Mere event collection amounts to a one-way conversation. Industry testaments concerning the need for central management are unanimous:

" . . . [C]entralized management is a must-have capability. Very few organizations have sufficient resources to replicate instances of management applications and operations personnel within each and every physical location that they do business.[25]"

"[S]everal physical sites within an organization can be managed from one location. Installation templates, configurable settings, logging, reporting, monitoring, updating, and much more can now be managed from a single location.[26]"

"After selecting controls, organize them so they can be managed collectively.[27]"

Central management not only makes the best use of limited resources and eases the maintenance burden for the security infrastructure; it also enables solutions that are much bigger than the sum of the parts. A true data privacy solution becomes possible through orchestration of the centrally managed mesh of technical security controls. An information overload solution can be realized without compromising security. The concept of measuring an enterprise's security posture now makes sense with central management.

At this point, the most comprehensive central management tool for the broadest array of network security infrastructure is the Internet Security Systems Proventia® Management SiteProtector™. ISS Managed Security Services also centrally manages an enterprise mesh of controls. ISS is also the only Managed Security Services Provider (MSSP) confident enough in its security to offer a guarantee on both security and service level agreements (SLAs). There are options available: maintain sole control of managing enterprise security or outsource it. Either way, an enterprise can still realize the **operational and compliance benefits** of centrally managing this enterprise mesh of controls. But it does not stop there. Both options provide further justification ammunition by enabling the corporation to document its security process.

DOCUMENTING THE SECURITY PROCESS

DOCUMENTATION = JUSTIFICATION

Though the relationship between the terms documentation and justification is not as strict as the heading above suggests, the terms justification and documentation are often used synonymously within a compliance context. Without documentation, corporations do not have much justification. Companies will not be able to justify their decisions without supporting documentation, and cannot demonstrate and justify strengthened internal controls without showing related procedural documentation. Neutral third-party validation cannot be proven without documentation. A track record of progress can only be proven through supporting documentation. Justification is a required step for compliance to prove an increased level of accountability and transparency. Documentation supports both accountability and transparency.

"You must justify and document all decisions.[28]"

"Document, document, document — Procedures can be followed only if they are clearly stated, and they can survive only if they are documented. Documentation supports accountability and transparency — who did what and when? What was the state of the system at a particular point in time?[29]"

"As a matter of good practice, documentation is considered essential for good control, and therefore lack of documentation would be cause for further review and analysis for compensating controls in any specific area under review.[30]"

*"**A documented control process** that will mature with time is a strong foundation to build a defensible case for compliance.[31]"*

PROCESS-ORIENTED SECURITY PROGRAM + DOCUMENTATION = DEFENSE

Just as in the documentation/justification relationship explained above, a solid defense can only be made if companies have instituted a well-documented, process-oriented security program. A central management tool can facilitate this security process documentation, outputting reports that support each stage of the process. An example of documenting the security process appears later in the paper.

"Organize these controls in a well-documented, process-oriented security program. This will allow you to create a defensible case to support the assertion that your company's control decisions were the right ones, given your unique situation.[32]"

A vendor-neutral security process helps companies judge, or compare, the relevance of any vendor's security management tool for demonstrating compliance. A tool that provides complete support for such a process carries a greater compliance burden for the company and bears much greater relevance to compliance efforts than one that only supports part of the process. As an example of judging the relevance of a vendor's security management tool, examine the vendor-neutral security process below, "Eight steps in the Vulnerability Management Process."[33] Proventia Management SiteProtector can help companies document each stage of this security process.

Figure 1: The Vulnerability Management Process

This particular security process provides stages for both vulnerability protection and correction. The eight steps of this process are listed and explained below:

1. **Policy** – the first stage where many (if not all) of the administrative controls are defined. Company, configuration and security policies all fall under this umbrella of administrative controls. The Policy stage is where companies:

"[D]efine the desired states for network and system configurations, resource protection and resource access.[34]"

Defining and documenting administrative controls consists of the majority of the compliance effort. Therefore, partnering with ISS Professional Security Services to serve as a trusted security advisor will alleviate the pain of the defining and documenting these administrative controls.

2. **Discovery/Baseline** – involves discovering the assets on the network and establishing a baseline against which to compare current and subsequent vulnerability protection and correction efforts. Identifying assets and clarifying the criticality of these assets helps guide both control selection and risk abatement efforts.

"An organization should identify all assets and document the importance of these assets.[35]"

"The Federal Information Security Management Act (FISMA) is largely an exercise in documentation, asset classification and discovery via vulnerability assessment. Although regulations can be distracting if the focus is on compliance rather than protecting data, when a best-practice approach is applied, organizations can improve their overall security posture and then readily demonstrate compliance.[36]"

Employing an asset-centric central management tool such as Proventia Management SiteProtector to document asset criticality and assigned asset responsibility, in addition to governing vulnerability assessments, combines threat, vulnerability and asset-related data all in one place.

"[T]he entity responsible for each asset or security process should be assigned and the details of this responsibility should be documented (see also 7.1.2)"

"In addition, ownership (see 7.1.2) and information classification (see 7.2) should be agreed and documented for each of the assets." (ISO 17799)[37]

3. **Prioritization** – Output from the Discovery/Baseline stage is used as input to help prioritize mitigation efforts. Central management tools, such as Proventia Management SiteProtector correlate and prioritize security event data into actionable steps, greatly facilitating this stage of the security process.

*"The challenge is to **focus on the most important things** and not try to checklist everything. **Wherever the most money and greatest potential for fraud exist**, that's where auditors will investigate first, and **where IT architects need to focus their efforts**.[38]"*

"Mitigation efforts need to be prioritized according to these factors:
- *The Nature of the Vulnerability and the State of the Current Threat Environment*
- *The Business Use of the Vulnerable Asset – Asset Inventory and Classification[39]"*

Logically, prioritization is most easily accomplished when the vulnerability, threat and business use data about each asset are all centrally located in one place, which Proventia Management SiteProtector accomplishes.

4. **Shielding** –As established earlier, the best way to shield vulnerable assets is via vulnerability protection. This type of security not only enables vulnerability protection and correction but patch management on the company's schedule as well.

*"**Use compliance as an opportunity to improve operational security** not only by defining assets and documenting the current state of the organization, but also by implementing control objectives that drive effective risk analysis and management."*

*"Organizations should **use compliance as an opportunity to implement technologies and processes that improve operational security** as well as providing support for FISMA and FIPS 199 compliance.[40]"*

5. **Mitigation** – The central management tool must also provide workflow and ticketing functionality as well. Why? What better place to begin the vulnerability remediation process than through the same tool that performs the assessment? Moreover, the same workflow and ticketing functionality can be leveraged for incident response purposes. Having the ability to group related security events into a single incident enables security personnel to focus on these incidents first, in addition to reducing event clutter and the potential for information overload. Proventia Management SiteProtector, working in conjunction with Proventia Management SecurityFusion™, provides this functionality.

6. **Control/Elimination of Root Cause** – In this stage, the security management tool conducts analysis in order to identify a pattern or trend associated with the asset vulnerabilities, and eliminate the root causes. This type of analysis requires flexible filtering and the slicing and dicing of data.

7. **Maintenance** – At this stage, compliance demands that day-to-day operational tasks be clearly defined and that roles, responsibilities and permissions be clearly defined as well.

"[A]uthorization levels should be clearly defined and documented."

"Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy."

"All procedures and authorization levels should be clearly documented.[41]"

In the context of compliance, segregation of duties is important because its employment and enforcement ensures that no one can hide his or her actions.

"Internal controls call for segregating duties, so there's no chance of someone being able to cover up wrongdoing.[42]"

Proventia Management SiteProtector supports segregation of duties in several ways:

- A flexible roles and permission model supports granular permission setting and custom role creation.
- Multiple consoles can be employed to physically separate roles across multiple machines. This way, each console could be assigned to a different role.

8. **Monitoring** – This stage monitors the security infrastructure for violations of acceptable use, vulnerability remediation and incident creation activities, and analyzes the stream of security events for questionable or other security-related activity. Monitoring provides an opportunity to report on improvements made throughout the security process, including reduced vulnerabilities as a result of mediation, and decreased incidents due to new security controls. Documenting a track record of improvement also strengthens justification and defense before the auditors.

"Continuous discovery and baseline steps and VM [vulnerability management] steps repeated as part of an ongoing process. Up-to-date vulnerability assessment and security configuration information is needed.[43]"

*"**Showing a track record of improvement** also will allow you to better defend your company's controls.[44]"*

MAPPING SECURITY MANAGEMENT REPORTS TO THE SECURITY PROCESS

Reports accompany each stage of the security process. See below for an example of how Proventia Management SiteProtector reports are mapped to the security process overall.

Figure 2: Mapping SiteProtector Reports to Vulnerability Management Process

CONCLUSION: SO, WHAT IS COMPLIANCE AGAIN?

In the end, compliance involves meeting a standard of due care, balancing legal and ethical concerns, addressing risk and justifying and documenting process and controls. Some helpful components for demonstrating compliance before the auditors appear below, and in a sense, these collective components define compliance.

Components For a Strong Defense:

- Adherence to the rising standard of due care via improved operational security. Proactive vulnerability protection is needed to augment (if not replace) reactive threat countermeasures. Some of the proactive vulnerability protection controls discussed were host-based Intrusion Prevention Systems, Network Behavioral Anomaly Detection Systems, Multi-Function Systems, Network Intrusion Prevention Systems and Vulnerability Management Systems.
- An enterprise mesh of controls with tiebacks to business processes and risk assessments.
- Justification Documentation for controls selection, guidance mapping, etc. This includes third-party validation for control selection, frameworks used in control selection as well as mapping framework requirements to controls selection.
- Documented security process verifying Asset Clarification, Vulnerability Remediation, Incident Response, Segregation of Duties, Workflow and Ticketing, clearly defined roles and responsibilities, audited security activity, as well as a demonstrated track record of improvement.

ABOUT INTERNET SECURITY SYSTEMS, INC.

Internet Security Systems is the trusted expert to global enterprises and world governments providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. ISS products and services are based on the proactive security intelligence conducted by ISS X-Force® research and development team — the unequivocal world authority in vulnerability and threat research. With headquarters in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 800-776-2362.

BIBLIOGRAPHY – PART II

1 ISO 17799:2005 (available for purchase at http://www.iso.org/iso/en/ISOOnline.frontpage)

2 ibid.

3 ibid.

4 ibid.

5 PCAOB Release No. 2005-009, May 16, 2005, http://www.pcaobus.org/Rules/Docket_008/2005-05-16_Release_2005-009.pdf

6 Gartner, "The Chief Information Security Officer's Guide to Compliance," 12 January 2006, ID Number: G00136911

7 "As Threats Evolve, Defenses Must Adapt," October 17, 2005, http://www.eweek.com/article2/0,1895,1871414,00.asp

8 "Viruses Get Smarter — and Greedy," November 22, 2005, http://yahoo.businessweek.com/technology/content/nov2005/tc20051122_735580.htm

9 "Norton Gets a Bit Less Secure," December 1, 2005, http://businessweek.com/technology/content/dec2005/tc20051201_834834.htm

10 "Lifecycle of a Vulnerability," http://www.iss.net/documents/whitepapers/ISS_Vulnerability_Lifecycle_Whitepaper.pdf

11 Gartner, "Select and Implement Appropriate Controls for Regulatory Compliance," 16 November 2006, ID Number: G00131086

12 Meta Group, "Securing Internal Networks: The Final Frontier," March 2005

13 ibid.

14 "Proventia offers advanced virus protection," March 20, 2006, http://www.fcw.com/article92607-03-20-06-Print

15 "Viruses Get Smarter — and Greedy," yahoo.businessweek.com.

16 Meta Group, "Securing Internal Networks: The Final Frontier."

17 Gartner, "Data Protection Is Less Costly Than Data Breaches," 16 September 2006, ID Number: G00130911

18 Meta Group, "Securing Internal Networks: The Final Frontier."

19 Gartner, "Understanding the Nine Protection Styles of Host-Based Intrusion Prevention," 27 May 2005, ID Number: G00127317.

20 "Defining the Rules of Preemptive Protection: The ISS Intrusion Prevention System," Internet Security Systems, http://www.iss.net/documents/whitepapers/ISS_Network_Intrusion_Prevention_White_paper.pdf

21 Meta Group, "Securing Internal Networks: The Final Frontier."

22 "Improving security in a dynamic environment," http://www.datanets.ro/network_security.htm

23 Meta Group, "Securing Internal Networks: The Final Frontier."

[24] ibid.

[25] ibid.

[26] "Vexira Releases Centrally Managed Security Suite for Windows," 5/3/2005, http://www.esj.com/vendor_news/article.aspx?editorialsId=493

[27] Gartner, "Select and Implement Appropriate Controls for Regulatory Compliance."

[28] ibid.

[29] Gartner, "Implement 10 Elements of a Good Control Environment to Address Compliance," 16 November 2005, ID Number: G00131264

[30] NSS 2005 Gigabit IDS testing, March 2005.

[31] Gartner, "Implement Security Controls to Comply With Section 404 of Sarbanes-Oxley Act," 7 October 2005, ID Number: G00127941

[32] ibid.

[33] Gartner, "How to Develop An Effective Vulnerability Management Process," 1 March 2005, ID Number: G00124126

[34] ibid.

[35] ISO 17799:2005.

[36] Gartner, "Findings From 'Security and Risk' Meeting: Augment FISMA Reporting With Technical Controls to Improve Operational Security," 4 April 2006, ID Number: G00139109

[37] ISO 17799:2005.

[38] IT Architect, "Crushing Compliance", 12.05, Vol. 20, No. 12, pages 25-26.

[39] Gartner, "How to Develop An Effective Vulnerability Management Process."

[40] Gartner, "Findings From 'Security and Risk' Meeting: Augment FISMA Reporting With Technical Controls to Improve Operational Security."

[41] ISO 17799:2005.

[42] Gartner, "Sarbanes-Oxley: An External Look at Internal Controls," August 2004.

[43] Gartner, "How to Develop An Effective Vulnerability Management Process."

[44] Gartner, "Findings From 'Security and Risk' Meeting: Augment FISMA Reporting With Technical Controls to Improve Operational Security."

Copyright© 2006 Internet Security Systems, Inc. All rights reserved worldwide

Internet Security Systems and Ahead of the Threat are trademarks, and the Internet Security Systems logo, Proventia, RealSecure and X-Force are registered trademarks, of Internet Security Systems, Inc. All other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

Distribution: General

PM-COMPWPv2-0706