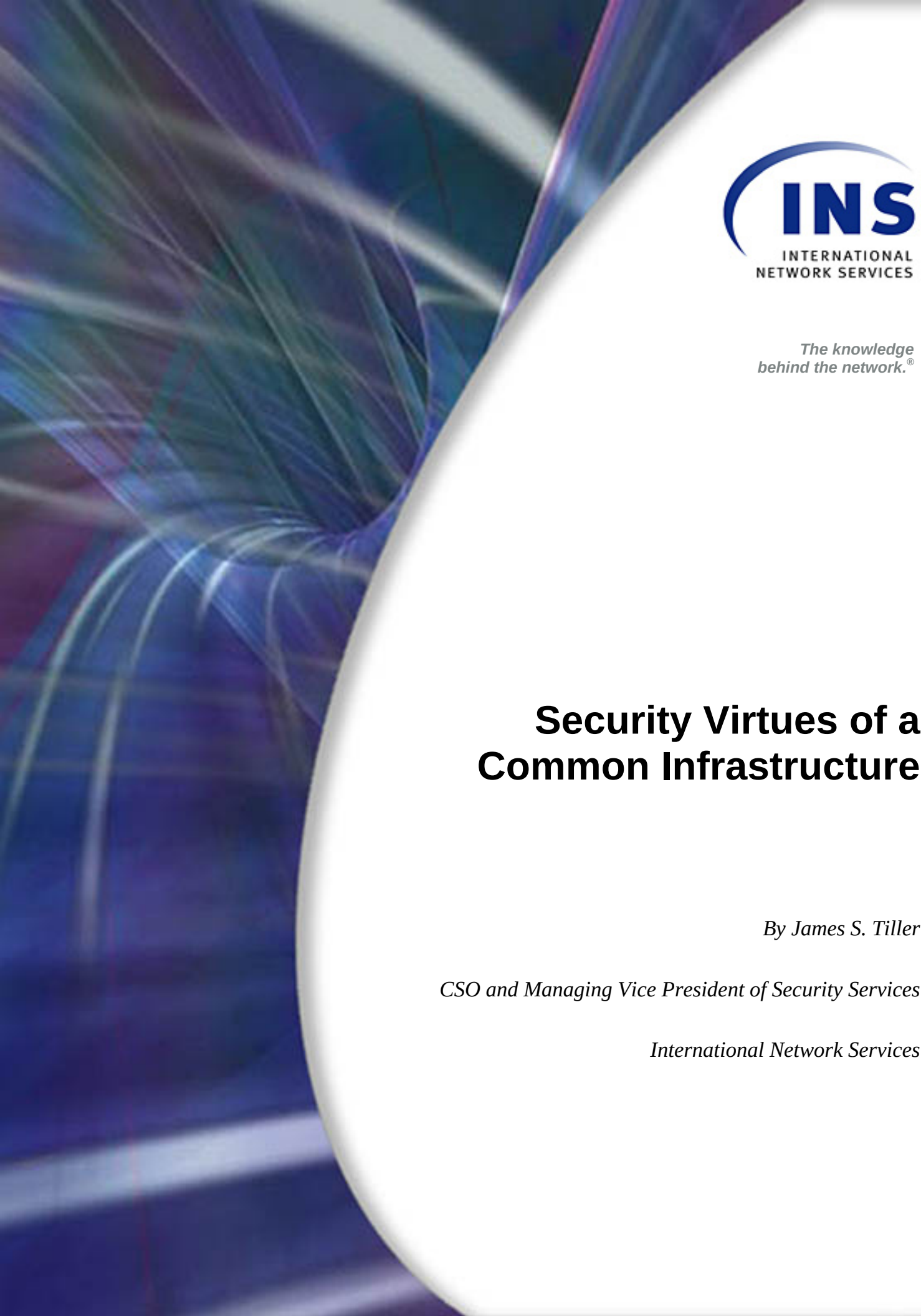

INS
INTERNATIONAL
NETWORK SERVICES

*The knowledge behind the network.®*

# Security Virtues of a Common Infrastructure

*By James S. Tiller*

*CSO and Managing Vice President of Security Services*

*International Network Services*

# Security Virtues of a Common Infrastructure

**By James S. Tiller**

## Executive Summary

IT organizations are faced with multiple regulatory requirements, constantly evolving threats, and increasing demands from the business to accommodate market dynamics. The need for greater efficiency and tighter investment utilization has proven to be challenging given the diversity and complexity of the typical IT environment.

Interestingly, it is the network that is reemerging as a valuable asset in the fight for meaningful and effective security. The network touches everything and as such provides a high ground in battle between business operations and the threats that seek to impair them. Threats take advantage of gaps that arise from complexity and inconsistencies in the technical infrastructure. However, the network is being utilized for proactive defenses by binding security logic, policy, and applications with its inherent capabilities in communications. No longer is the network just a conduit for attackers, but rather the enabler of policy, offering frontline command and control right where it is needed most.

The proliferation of tools has sought to bring consistency to security oversight. In contrast, the network offers the uniformity we desire in addition to extending the reach of management and visibility. By incorporating security intelligence into the network, enforcing policy and dealing with those who do not conform, the enterprise security strategy quickly transforms from one of reaction to one founded on offence.

Cisco is the first to offer an aggressive approach to coupling security with the network, extending the reach and depth of control, placing security squarely in the face of threats.

# Introduction

Information security is a significant challenge facing all organizations. The combination of the increasing number of sophisticated threats and rigorous compliance requirements has added a new dimension to how information security is visualized within the business environment. Prior to the 21st century, adversaries were malicious programs and unethical individuals rendering early Internet-facing systems useless in the face of denial of service attacks and other network layer onslaughts. By today's standards, those attacks were primitive and merely an annoyance when compared to the destructive force impacting the Internet today. The introduction of regulations affecting the security of information has not only raised awareness of a global issue, but has forced companies to make significant investments in meeting legal demands.

The evolution of threats and regulations has placed organizations squarely in the sights of the unlawful and the law. Now the battle is being fought on two fronts. The first front is fending off attackers and managing the plethora of vulnerabilities they seek to exploit. The second is addressing the demands of regulations and ensuring compliance in the face of significant penalties. These challenges are exacerbated by the existence of a highly competitive business environment that demands efficiency and effectiveness

The continued evolution of complex applications and comprehensive infrastructures, even while the Internet bubble was still deflating, has forever bound business to technology. That business-enabling technology has allowed companies to perform more aggressive services and to produce more competitive products. However, the beneficiaries of the added capability have also unwittingly acquired the greater responsibility of protecting information and the systems which make its use a reality.

Protecting information from a sea of threats has materialized as extensive new processes, procedures and technology designed to ensure a well fortified security posture. However, it is technology that has reigned supreme as the primary focus in fending off the inexorable attackers. In an effort to quell the vast dynamics of exposures, the vulnerabilities that make them a reality and the threats that seek to exploit them, many organizations look to point solutions that represent the latest in defense capability. However, while on the surface the practice of implementing point solutions ensure that specific controls are employed, it lacks the broader security virtues found in a comprehensive, homogeneous infrastructure. These valuable, but rarely highlighted security virtues begin to materialize when a common security thread exists within the infrastructure.

In short, complexity and inconsistency are information security's nemeses. They introduce gaps in the fabric of visibility and capability, potentially leading to unwanted exposure even in the most secure of environments. It is the objective of this paper to introduce the security and business advantages that surface when a common platform is leveraged throughout an infrastructure and to demonstrate how this philosophy applies to those elusive, yet valuable attributes of information security.

# Complexities and Inconsistencies

The ability to ensure a sound security posture is challenged with the introduction of complexities and inconsistencies in the environment. Complexities surface as the scale and scope of the environment expand and as specific applications, processes, services, interactions, and users with different requirements are introduced. For each new characteristic introduced into the infrastructure to accommodate a myriad of business requirements, the complexity of the environment increases exponentially. Furthermore, the expansion of the infrastructure to support a business requirement almost always requires the introduction of new or different technical components. These can materialize as new software, operating systems, or platforms.

Complexity is inherent and unavoidable in today's corporate IT. It is not uncommon for an IT department to oversee thousands of systems and a multitude of unique applications to support the demands of the business. The pressures on IT executives to control costs, increase effectiveness and provide a feature-rich collection of services tend to promote greater complication through the introduction of disparate technologies. Therefore, from the customer's perspective the use and management is more efficient and effective, while under the surface hides a web of intricate, diverse technical interactions challenging the ability to provide a meaningful security posture.

The result of the issues outlined above impedes the ability to manage the security environment in a comprehensive manner. Without a common security foundation, an organization must inspect the state of security controls individually, forcing the interpretation of broader implications for the security posture overall. Therefore, an organization must compile different information to determine the state of the security posture, potentially leading to inaccurate conclusions of risk or level of compliance. Comprehensive and continual management of information security are critical to establishing a meaningful security posture. Consistency in the infrastructure is a significant ingredient in achieving the much needed management capability.

## *Security's Nemesis*

Security in the technical domain is founded on a defense in depth strategy. The layering of security controls in a methodical framework provides overlapping protection and offers a common thread throughout the infrastructure. Historically, this need has not been pronounced for typical IT services. Applications processed information, routers forwarded packets, routing protocols converged, and network and systems played their roles to ensure that the organization functioned effectively. The consistency and ability to provide services is based on the processing of data at each layer and stage, in addition to its type, format, and state. For example, an MPLS network transfers data and provides services to upper layer devices and applications. As the use of the MPLS network moves further from the core and closer to the edge, the relationship is less important and virtually unidentifiable. In contrast, within the realm of security, the relationship from core to edge is critical.

The role of traditional IT components is to play their part in the larger picture of the services being offered. Differences in their individual functions have little impact on the combined objective of the network. Conversely, it is necessary that relationships exist at all layers to facilitate a comprehensive approach to securing the environment. Therefore, although parts of the IT environment are instruments tuned to the same key, sound security is a harmonic symphony composed through collaboration at all levels.

To further demonstrate, consider a secured facility with gates, guards, cameras, and multiple doors and locks protecting a single room. In addition to performing their individual roles in maintaining a level of local security, they support one another, increasing the resistance to exploitation. If the gate is penetrated, the guard will provide the next layer of control. In the event the guard is overwhelmed, cameras will alert others, and so on. Simplicity and commonality in the strategy minimizes or eliminates gaps between the various controls points in this example.

In contrast, in a complex technical environment, data and sessions interact in ways that increase the potential for gaps in security resulting in expanding opportunities for exploitation. These gaps can materialize between firewalls, applications, services, or at user access points; each representing a point of exposure to unwanted influences. When inconsistencies are introduced, the issues with security are exacerbated. As data is acquired and processed in a multitude of ways to produce products and services, each step in activity being performed by unique elements acts to intensify the complexity and further expand the gap, and more importantly, affect the ability to control, manage, and troubleshoot security related events.

The concept of a defense-in-depth strategy combined with the larger implications of a common technical environment is best described as a security thread. A security thread defines the ability of an organization to ensure the collaboration of multi-layer attributes within a defense-in-depth strategy throughout the environment.

## *Setting a Standard*

Given a complex environment is unavoidable in today's business, one method to compensate for the gaps and exposures is the assurance standardization provides. Standardization by no means is a new philosophy and is regularly employed as a best practice for IT organizations. While this is also true for some in addressing the allocation of security related technology, it is usually relegated to a specific realm or layer in the security architecture. For example, a company may standardize on a firewall platform, an anti-virus solution, or an intrusion detection system, but rarely are common security attributes applied consistently across multiple domains of an infrastructure.

That lack of consistency across the enterprise can represent a challenge to the establishment of a business-enabling security capability. Interestingly enough, much of the security-related activity being performed today for regulatory compliance is in many ways compensating for the variety of technical solutions that have evolved over time.

To increase security and reduce exposure of information at various points within the network, a common security presence and awareness at each layer must exist for all other layers in the system. We accept this strategy in many other areas of IT. For example, directories accessible by many applications and systems are used to authenticate users. Identity management solutions provide credentials to users that are applicable to many disparate systems and applications. We are seeing authentication at the network layer, such as 802.1x and VPN access being leveraged to authenticate and authorize use of downstream services. The closer the interaction between the layers of data management is, the more it does to promote consistency and simplicity, enhancing security overall.

## *Silver Bullet?*

A security thread can be realized by use of a common system architecture or a combination of like attributes based on an overall strategy. Today, many, if not all networks are heterogeneous from years of combining point products, each performing what they do best. However, any advantages of layer-specific focus are countered by the proliferation of gaps, management woes, lack of investment predictability, skill gaps, difficulty in enforcement, and unclear visibility. To compensate, numerous tools and processes have been introduced to manufacture consistency to address these challenges.

The argument for point products was originally based on the reality that no comprehensive technical solutions existed. Security was nebulous at best and entrepreneurs sought to offer products to address the greatest points of pain. However, as the sophistication of systems and the threats to them increase, point solutions fall short in supporting broader implications of security.

"There is no silver bullet" and "Technology is not the only answer" are well-known sayings in the security industry. We hold these truths to be self-evident, yet they represent a contradiction in our actions. For example, based on industry surveys, 99% of companies have implemented anti-virus solutions, yet virus and worm-related impacts rank as some of the highest in financial losses. Putting aside the availability of signatures and running scans, which are attributes of the specific solution, clearly worms are taking advantage of gaps in controls and leveraging networks and services at all layers to wreak havoc. What if the same strategy for anti-virus were enabled for all nodes within a network, each using a common approach to identify, isolate and eradicate the threat? Every layer in the network, from switches, routers, and load

balancers to operating systems, middleware and applications would be speaking the same language, applying their own enforcement in unison at the layer they service. Blue-sky thinking? Today, yes. Tomorrow, no. The emergence of mutli-layered virus management with access scanning and quarantining is already being seen. In fact, while virus management has evolved, some have begun to leverage the idea to extend to vulnerability management. For example, Cisco's Network Admission Control (NAC) utilizes the combination of network and software elements to investigate systems prior to entry into the environment. Cisco's approach to security is the best example of creating that elusive security threat throughout the enterprise. The result is greater efficiency in managing services, such as access, in the light of security demands and business requirements. Moreover, the added visibility and compressive management provides greater confidence in the oversight of controls, their impact to business operations, and the wherewithal to enact decisive changes.

# Security Confidence

Knowledge is everything and the ability to act upon information is essential to sound security. Gaining insights into threats, vulnerabilities, activities and incidents combined with awareness of the state of systems and security controls provides for greater visibility into the environment. Additionally, the ability to respond to information in a decisive manner with confidence is paramount. Fundamentally, security at its very core is awareness and the capacity to enact change effectively and comprehensively. Clearly, these added advantages are not feasible without a common security capability throughout the environment. Point solutions are islands weathering the storm of attack with limited options for collaborative management and defense. In contrast, a common security-aware infrastructure will establish meaningful bridges between different elements of the network, greatly increasing defensive options, control, and visibility.

## *Security Visibility*

Arguably, the level of security realized is directly related to intelligence. Information about the state of the environment, potential threats, vulnerabilities, and unwanted activities within the infrastructure are fundamental to all aspects of security. Without visibility into the state of the environment, many, if not all other parts of the security program are immobilized. For example, policies define the expectations of employees, partners, and even system operations in meeting your security needs. Without the visibility into the environment to ensure the policies are being followed and enforced, the policy is rendered nearly useless. Incident response processes are inherently at the disposal of the ability to detect, identify, and qualify events. Threat and vulnerability management is ineffective without intelligence about the network in making determinations concerning the applicability of newly identified vulnerabilities and what actions must be taken in the light of the infrastructure's status.

Visibility and awareness of the environment is essential and the closer to real-time the better. Of course, some hard lessons have been learned. Intrusion detection systems became the next big wave of standard security technology after the firewall revolution. However, the added information on the state of security activities – sometimes in the form of an avalanche – overwhelmed many. Nevertheless, IDS ushered an era of increased desire to know what's happening in the environment.

A common architecture, effectively supporting a common security thread, provides the facility to obtain diverse information quickly and to visualize the broad implications in alignment with policies and criticality. Commonality inherently provides for seamless representation of information from disparate technical sources, e.g. routers, firewalls, switches, work stations, servers, etc. It promotes greater visibility through the coordination of information gathering founded on a standard interpretation and production. When external intelligence and information about the state of internal systems is combined with a common strategy at all layers, policies defining the security posture can be enforced from one end of the spectrum to the other.

Finally, with a consistent approach and capability of extracting information from the environment, the ability to report against metrics and align those metrics to the business strategy is substantially increased. The embryonic stages of this philosophy can be seen in Return on Security Investment (ROSI) strategies. Unfortunately, without an overarching IT strategy that is security aware, these initiatives will suffer and remain open to interpretation.

### *Actionable*

Unfortunately, it is not enough to speak the same language. When a common infrastructure is introduced we begin to realize some significant advantages. As discussed above, visibility is critical to security. However, once obtained, the ability to enact changes with confidence, whether in an emergency situation or otherwise, becomes the crux of security. It is not enough to simply tie information together and distribute policy changes. One must ensure those changes are sensitive to a given system's state and role within the security architecture. Moreover, policies must be actionable. The objective is having the ability to learn a system's posture, compare it to established policies, enforce controls for access and authorization, and associate them with data and services.

Not only does this provide for immediate change and implementation of controls in an automated fashion, but is also significantly reduces risk because unwanted entities are managed. To demonstrate, the time between the publication of a vulnerability and the availability of an exploit is decreasing rapidly. What was once months and weeks has become days. According to reports from Symantec in 2005, the time between awareness and exploit has diminished to less than five days and some feel that soon it will be measured in hours. Historically, battling vulnerabilities meant you had to identify and understand a vulnerability to counteract the potential threat through remediation. With the visibility and management advantages a common security-aware infrastructure provides, it is possible to instill an added layer of confidence by proactively and comprehensively investigating the existence and status of controls and not simply whether a patch has been installed.

Interestingly, an alignment of IT and process are beginning to appear in the realm of security. Today, we have the emergence of service alignment, as with ITIL, and are beginning to see the treatment of IT in the form of security services. Business logic is being employed to enact change in IT based on a business services strategy. Security is following this trend at an accelerated rate. As the infrastructure takes on more security capability, IT management will start taking advantage of enabling characteristics and employ business logic to support dynamic and meaningful change in the environment to address the growing challenges of security. Therefore, with a common security thread through the infrastructure, the use of business strategy-aligned metrics to measure success and to automate those functions by leveraging proven business process can move from the whiteboards to reality.

## Omnipresence

Clearly, a consistent approach to security at all levels in the environment offers significant advantages. It was once acceptable to allow access based solely on IP address. Then came authentication, and soon that was tied to IP address in an effort to offer compensating layers. Now those times have long passed and it is necessary ask some basic questions to establish trust. Is the user being authenticated originating from the expected source? Is their system carrying a virus? Are they adhering to established policies? Do they employ best practices? Are they using authorized services? Is the data they are accessing meeting predefined classification strategy? Finally, how is the infrastructure supporting these attributes from stem to stern?

Ironically, the role of the network in regards to security has been relegated to the perimeter. In some cases, the core networking environment has sought to employ technology originally designed for the perimeter to

enhance the overall architecture. Over time, the network has taken a back seat to higher level interactions, such as PKI, identity management, application security, patch management, and virus controls. Nevertheless, it is the network that is emerging as a meaningful tool in the fight against *in*security.

The network is the one constant in the IT space – it touches everything. It connects and feeds the body of the business as a cardiovascular system, supporting applications and systems like organs offering services to the overall entity. It was once enough for a network to respond to changes and reroute information ensuring quality of service and performance. Now it is emerging as an immune system for protecting systems by closing holes, attacking infections before they spread, and offering a platform for communicating higher-level information to all those who participate.

It is within this context Cisco has taken the initiative. Arguably, as one of the most pervasive networking products in the industry, Cisco has seen their extensive adoption as an opportunity to inject a new era of information security by helping to solve some of the fundamental challenges of security. Cisco's Self-Defending Network (SDN) strategy is representative of how security is going to evolve in the technical realm. The intelligent networking is founded on the principle of binding the network and applications together in light of business processes and policy.

As mentioned above, a common security thread will help to ensure that the controls of a given layer work in concert with the controls applied at other layers. This full spectrum approach can be enhanced by weaving security services into the network. Applications and systems can work together in a coordinated manner without the gaps inherent in any complex infrastructure. Moreover, given that any element within an environment can become a point of attack, each of them must also be a defensive point. Consistency offers synergies in applying defensive tactics based on a strategy that is aware of the status and role of a given system within the environment. Cisco's SDN solution provides the much needed security thread, linkages between applications, systems and the network offering more visibility, enforcement, management, and confidence.

## Business Flexibility

One of the more challenging aspects of information security is the ability to enact change to support business needs while not adversely affecting services or increasing risk for the organization. The goal is to have a clear perspective of what is the capacity for change within the infrastructure, the extent to which the change can be employed, and to validate that it meets the demands of the business without compromising the desired level of security or compliance.

Typically, a change is planned, designed and implemented long before the security implications are identified. While this is not the case in some scenarios, it is the reality for most. The belated focus on security is the impetus for many reactive services, such as security assessments, risk analysis, and vulnerability tests.

Over the years, the infrastructure has been designed and implemented in a manner that seeks to facilitate change. Technologies such as ATM and MPLS are perfect examples of sophisticated solutions offering a multitude of services that can be changed according to business needs. Comprehensive provisioning and management solutions allow these technologies to bend in the waves of change.

In contrast, security is far more rigid. Policies are defined, implemented and managed. When a change occurs in the business process, the policy must be investigated and then translated to the infrastructure. Sometimes this forces the introduction of new point solutions which are potential propagators of complexity and inconsistency. Security intelligence, when introduced into the network, can be designed and managed much like we design and manage MPLS networks. Just as a network device and supporting systems may

use a common language for provisioning, management, troubleshooting, and monitoring, a common approach to security provides for many of the same advantages.

## Speaking to the CxO

Traditionally, Return on Investment (ROI) is associated with the cost of acquiring, implementing and managing solutions to support various services that produce more than they consume. The ability to maintain those services, such as uptime, performance, and scalability, is an indication of efficient use of those investments. At the highest levels, IT is part of an overall strategy to improve shareholder value and corporate image by ensuring productivity, improving asset utilization, and decreasing costs (or building efficiencies) for production. These can be aligned to the business, such as building customer intimacy, reducing errors, acquiring and retaining customers, improving customer satisfaction, and addressing new market opportunities.

With regards to ROSI, many of the same business demands exist. However there is more obscurity with what constitutes an actual return or what is being performed in the realm of security to meet those higher business imperatives. Most see security as an insurance policy, and this is usually the case. At its most basic level, ROSI is managing costs. In some very rare cases, it may be possible to demonstrate that a security investment has allowed the business to offer specific services that align to business objectives and in turn acquire revenue. For example, a customer community may be obtainable if a smartcard enabled PKI solution were deployed to instill an increased level of trust and efficiency for the clients, setting the company ahead in terms of competitive advantages. However, these benefits are rare and short-lived.

An example of building efficiencies can be expressed as an identity management solution. It can allow users to perform self-administration for password resets, potentially eliminating what industry reports say constitutes 48% of helpdesk activity, translating into reduced helpdesk staff. As far as investing to avoid future expenses, an automated patch management system could help compress the time window between vulnerability and exploit, introduce efficiencies, and ultimately reduce costs associated with vulnerabilities.

The reality is ROSI is essentially cost management. You can invest in security to build efficiencies that translate into reduced expenditures in other areas over time or you can invest in security to reduce exposure of future costs, such as those associated with vulnerabilities or incidents. Also, expenditures in the light of cost avoidance begin to include threats from regulatory penalties, something much more tangible to the board of directors.

Within the context of cost savings and avoidance, a common security thread throughout the infrastructure offers the benefits in management, visibility, control, and enforcement. Each of these attributes combines to build efficiencies in process, but more importantly they build confidence in proposed investments. A greater understanding of the state of the security environment allows more predictability in the scope and depth of proposed changes, in addition to understanding their impact on the security posture.

### *Security Downtime*

One of the most prevalent arguments for ROSI falls in line with traditional industry standards for downtime. What once was the oversight of system and network outages now includes the potential impact of threats, such as worms and all they imply. For example, if an IT service is not available, the business does not differentiate between a circuit going down and a worm consuming resources – it is simply unavailable. However, thanks to regulations, customer satisfaction, and shareholder value, security-related outages have a greater potential for broader losses. In the event of a circuit failure rendering a service unavailable, there is little concern over the integrity and implied protection of private information. In contrast, in the event a service is rendered ineffective by a worm, there exists the added concern of exposure.

**Table 1 - Example Impact**

| Challenge | Impact | Traditional IT Concerns | Additional Security Concerns |
|---|---|---|---|
| E-Commerce Site failure due to poor controls for website application. IT related impact = $41,400 | Inability to process transactions for 3 hours in peak time. Assume number of transactions in a given value x value per transaction (1000 per/hr at $12.65 ea. = $37,950) in potential losses. (This is putting aside statistical analysis and customer reacquisition). | Requires 12 employees for 3 hrs. to rectify, 3 employees 12 hrs to apply additional controls, 5 employees for 2 hrs to patch software, 2 employees for 2 days to update total application package, one employee for 3 days to audit controls. Result, 138 man hours. Assume $25 per/hr loaded costs (no overtime) = $3,450 | Almost 3 weeks later, it turns out the vulnerability in the application allowed an attacker to utilize a valid account for purchasing and decrease the predefined cost of equipment for sale. It was only when they got greedy that they caused a fault condition and the application failed. Result, $86,421.98 of product was sold for $86.42 and shipped to a "resender" in Atlanta, GA, from there it went to Belarus. Gross product related losses=$86,335.56. Additional results, existing customer received bill for $86.42, raised suspicion and forced a public exposure, stock drops 3%, recovers to -1% in four months. |

Demonstrated in Table 1, a typical outage of a website for a short duration due to suspected application development issues resulted in modest estimated losses of $41,400. However, in the light of a security incident, those losses more than doubled with the added concern of not knowing what could have happened beyond the evidence obtained. It is not uncommon for organizations to invest heavily in uptime controls and systems, but not associate a level of equal importance to the security of that service. The example demonstrates avoidable costs brought on by a lack of sound security investment.

The challenge many experience with the above scenario is that it is founded on opportunistic and unpredictable events, raising questions about the validity of the conclusions. However, over time, more empirical data is being collected that provides more evidence to the reality that such an event ***will*** occur, not ***may*** occur. Therefore, vulnerabilities can begin to be tied to realistic risks and ultimately to costs.

So how does this relate to a common, security-aware infrastructure? While the example is relegated to the Internet infrastructure, it can be readily and correctly concluded that with greater visibility into the infrastructure the example organization not only could have lessened the impact, but also could have provided confidence in remediation and the understanding of what may have occurred. Moreover, the post-mortem analysis of the event would be greatly enhanced by the synergies within the architecture. Finally, armed with a common approach, it is feasible that the enhanced awareness of the state of controls could have allowed them to identify the vulnerability early, avoiding the entire scenario altogether.

With more industry alignment of risk versus vulnerability, the infrastructure can provide comprehensive reporting options to determine where threats were mitigated, furthering the association to cost avoidance. Finally, the added visualization and control capability provides for investment focus, as opposed to spending more money to perform a detailed analysis to tell you what you already expect.

## *Regulatory Direction*

So far the implementation of compensating security controls has been an option. Organizations have taken one of three routes: avoidance, transferal, or acceptance. Avoidance can be construed as doing something about the problem. This can include anything from investments in targeted controls to the approval of an initiative to reduce risk. Transferring the problem can be best described as shifting responsibility and related liability to a third party, such as a managed security services provider. Finally, acceptance is the conclusion that the cost of resources required exceeds the potential losses or impacts. For some, simply accepting the risk and hoping for the best is the modus operandi. In fact, for many, rarely is a detailed analysis performed

to make one of these three basic determinations. The lack of funds to support yet another evaluation, the complexity of the process, and the knowledge that security changes will be broad and expensive have combined to force many to simply accept "security through obscurity" philosophies.

However, with the introduction of regulations, the choice regarding security controls is for most no longer an option. Companies are faced with investing in security controls for compliance purposes, and some are taking the action as an opportunity to enhance security as opposed to merely meeting compliance.

The security virtues of a common architecture speak directly to compliance. Moreover, the level of compliance will be easier to maintain, to scale to changes in the business, and to address new regulations as they emerge. Although security regulations appear to be unique, they are cut from the same cloth. The ability to protect information, even in the light of technical advancements, still relies on fundamental best practices. Therefore, a common security capability and thread throughout the network will allow for the implementation, management, and oversight of security-related mechanisms in a consistent manner. At this point, the general security advantages of a common architecture move from technical opportunity to business enablement.

A security-aware network – one that touches and services everything - is where the greatest advantage for compliance resides. For example, while Sarbanes-Oxley is extraordinarily comprehensive, the ability to report on security (e.g. sections 404 and 302) and general controls speaks directly to the abilities of the network. While most are focusing on application controls and assuring the validity of transactions, the real test is in the network's ability to ensure that data remains confidential and free from exposure – the network can be the strongest asset or the weakest link. Moreover, the ability to report on security is having the confidence in the controls and visibility into their status.

The existence of a security-aware infrastructure can be extraordinarily valuable in the light of regulations. Many organizations today are investing in the development of a common security management architecture. The goal is to facilitate a consistent approach to policy and process that will ease the compliance burden of proof in addition to having a framework that can be easily applied to new regulations. The same objective holds true for technology. A security thread binding networks, applications, services, and management has the potential to offer greater compliance oversight with less need for modification to address emerging regulations. The ability to understand the threat and vulnerability environment, determine the status of controls, and validate policies are being enforced throughout the technical infrastructure significantly reduces the effort associated with technical compliance.

## *Slippage and Expense*

If an organization is faced with compliance challenges, a significant percentage of IT budget must be committed to perform an assessment of existing capabilities to determine gaps and the eventual development and implementation for remediation. With the complexities and inconsistencies in today's infrastructures, these costs will increase over time as each audit is performed and gaps are closed. Historically, security-related costs have been roughly 2%-4% of IT budgets. With the onset of regulations, that has increased to nearly 15%. For many, these investments are targeted point solutions with limited integration and increasing emphasis on implementation. As time passes, inconsistencies will prevail, forcing more expenditure due to security slippage.

Security slippage is reflective of many IT realities. There are points in time when business objectives, service changes, or customer demands ignite interest and focus. Today we see unparalleled interest in security because of regulatory demands and the increased impacts of the threat environment. However, traditionally focus wanes over time and moves into maintenance mode. Shortly thereafter, many solutions begin to fall victim to apathy. In the realm of security, this happens all too often and at some point during

the decline in focus, an event occurs, such as an attack or business change, and once again, security becomes the focus requiring more investment to increase the security posture (Figure 1).

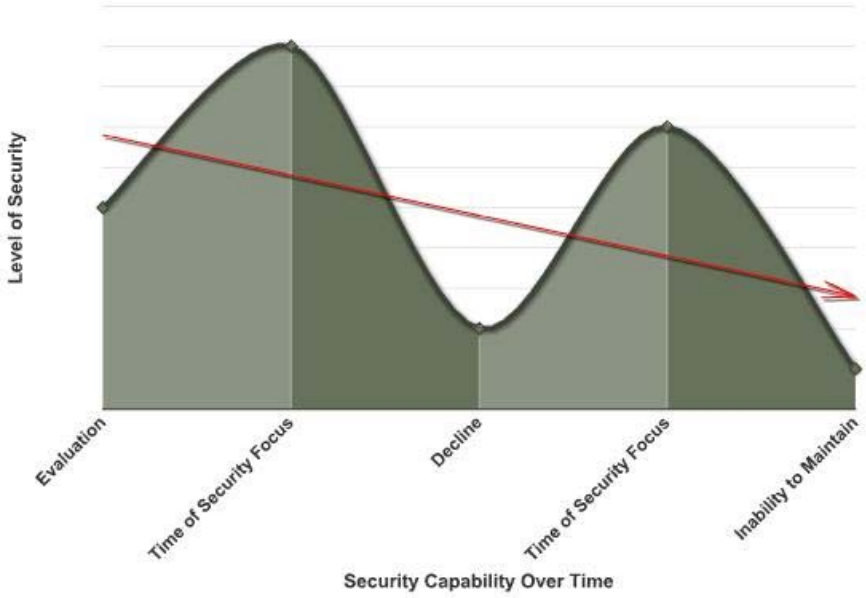


**Figure 1 - Security Slippage**

Unfortunately, the capabilities tend to diminish over time while investments seem to increase. Inevitably, the long-term decline will collide with a significant change, such as a new regulation, a merger or an acquisition, or a new business imperative, which translates into an investment "balloon" to employ broad changes to the security posture.

The important element to avoiding slippage, especially with regards to compliance, is to have a simple, yet effective method for managing the security of the infrastructure. Many security management programs fail simply because they are too complex. Usually the process is the cobbling together disparate unrelated information to make determinations on the status of the environment. As changes occur in the infrastructure the excessive number of processes for collecting and evaluating dissimilar information must be changed as well. To add to the malaise, the entire approach is typically opportunistic in that information is collected based on the fact that it can be collected, not necessarily if it applies to the broader perspective of security and compliance.

Clearly, the existence of a security thread and the implied capabilities facilitates greater efficiency in collecting meaningful information and the enhanced ability to qualify that information against the overall status of the organization. It is this which represents one of the significant, but less discussed features of Cisco's approach. The intelligent networking is founded on the acquisition of information on the state of controls and the policies that guide them. Moreover the ability to compare and act on results in an automated fashion speaks directly to efficiencies in the managing security. Given the advent of automation and action orientation of the strategy, the risk to security slippage is considerably less, saving valuable time and resources over the long-term.

## *Crossing Over*

The long-term affects on security posture and related investment cycles, while unpredictable, are directly related to the security strategy employed. Strategies fall into three categories: point solutions, generalist strategy, or common architecture.

Point solutions speak not only to technical implementations and best-of-breed products, but also to quantify security culture and organizational hierarchy. For example, a global organization may have 200 firewalls managed by three different security groups distributed by primary corporate geography. In addition to the potential for different product uses, differences may exist in practice. Interestingly, any differences are purely founded on reasoning well outside of information security. If security were paramount, undoubtedly a consistent strategy would be more effective.

Many organizations have adopted a general strategy in addressing security in a corporate-wide philosophy. Consistency is collected in groups of people, process, and technology with an overarching common framework. This allows companies to apply prescriptive actions within a given domain with an overall approach. However, with the lack of a common architecture that provides a security thread throughout the infrastructure, it will remain virtually segmented. Using the example above, a generalist strategy company would deploy the same firewall product and have detailed, global processes for all management. However, those consistencies exist only within the firewall domain and are not pervasive.

When a common architecture exists, the availability of enhanced visibility, increased consistency, and relationship to required controls provides for long-term efficiencies. While these efficiencies provide for more security control and alignment to business requirements, such as meeting regulatory challenges, they also help control investments.

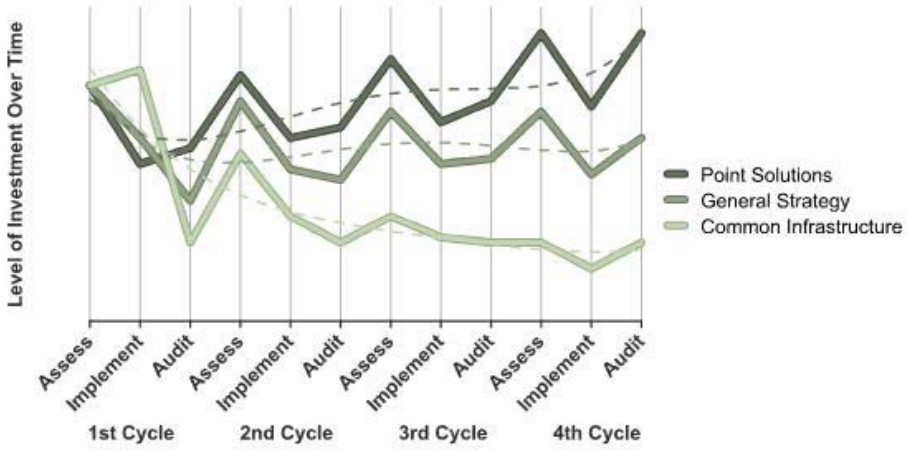


**Figure 2 - Investment Over Time Depending on Strategy**

As demonstrated in Figure 2, the investment lifecycle is related to each strategy type. Assuming that companies follow the typical assess, implement change, and audit controls regularly over time, the consistencies inherent to the strategy will translate into operational predictability and ultimately more controllable investments. Depending on your environment, the implementation of a common infrastructure may be more expensive than implementing point solutions or the gains in bulk product and licensing price breaks as seen with general strategies. The added expense is due to the pervasiveness of a common solution. In other words, to obtain a common thread, changes to seemingly unrelated infrastructure elements will be

required. Initially, this is seen as an enormous undertaking and expense. Most organizations have difficulty in demonstrating long-term value because of previous large project failures or the promise of hidden costs. However, the virtues of a security-aware network unmistakably speak to the needs of the business in understanding the state of the security capability with regards to defensive capacity and compliance, while demonstrating long-term savings.

For point solutions, costs will increase over time due to slippage, inconsistencies, and complexities. General strategies are becoming adopted more readily because the investment strategy and security strategy begin to align and plateau as long as the business dynamics are not excessive. In contrast, a common infrastructure offers mid-term reductions and levels off much lower while supporting business transformations. This is founded on the principal that the network is a constant throughout the organization. It is also based on the fact that a common infrastructure will allow for simplified management, greatly reducing the evolution of gaps in controls, which typically materialize over time forcing spontaneous investments. When management is simplified it is more apt to being correctly and consistently performed, allowing the identification of gaps before they become crippling vulnerabilities in the posture.

With more consistent controls and visibility, the process of assessing the environment, identifying gaps, applying change, and ultimately auditing those controls becomes much more efficient. Putting aside the increased security and ability to enact change decisively, a common architecture provides the tools necessary to report on compliance in meaningful terms to business owners.

An additional compelling argument is the reality that introducing a common infrastructure falls within the scope of the other strategies for implementation. Specifically, each strategy is governed by product lifecycle management. In spite of strategy differences, the products that make up the infrastructure can be acquired based on the traditional technology refresh cycles many IT organizations abide by. Additionally, as seen with general strategies, there are savings opportunities when purchasing solutions. For example, by utilizing a single vendor one can implement in a phased approach meeting internal cycles while taking advantage of comprehensive pricing models. Arguably, this is more effective over the long-term and simplifies future modifications.

## *Security in Business Terms*

Finally, one of the most valuable benefits of a common security infrastructure to the CxO community is security services management. Introduced above, this elusive advantage is the alignment of security in the terms of services. The recipe for successful service oriented security includes three main ingredients: the definition of a metrics strategy, metrics alignment, and key performance indicators (KPI).

The security metrics strategy is an association with key elements of the business strategy and measurement processes. This can be related to the areas of a balanced scorecard and the management of the business based on multi-dimensional characteristics. Once tied to the business objectives and management practices, the metrics alignment to security services takes place. For example, security may be oriented in the form of services, such as vulnerability management and incident management. While these services are different in practice, they may use the same infrastructure elements and base processes (for example, firewalls and change control). When services are defined, they can be measured based on KPIs that expose efficiencies or weaknesses. Most associate KPIs with number of attempted attacks, blocked viruses, or number of patches deployed. Unfortunately, it is difficult to communicate to upper management that security is participating in the support of corporate strategies, such as new customer acquisition or error reduction.

The reason for the gap is relatively simple: there is a lack of a consistent infrastructure to support broader insights. The domain-based security architecture supports tactical reporting because merging with dissimilar data is highly complex and open to interpretation.

Today, many companies are seeking to bring an overarching strategy to security, yet the segmentation of the technology into security domains challenges the ability to comprehensively and consistently report on the security posture in business terms. When a common infrastructure is introduced and all the capabilities are provided, the gap between people and process and technology begins to vaporize, allowing security services to be governed based on business needs. Moreover, those needs may vary depending on department or geography. In this event, the services can be tuned to reflect the level of risk and security offered to that entity.

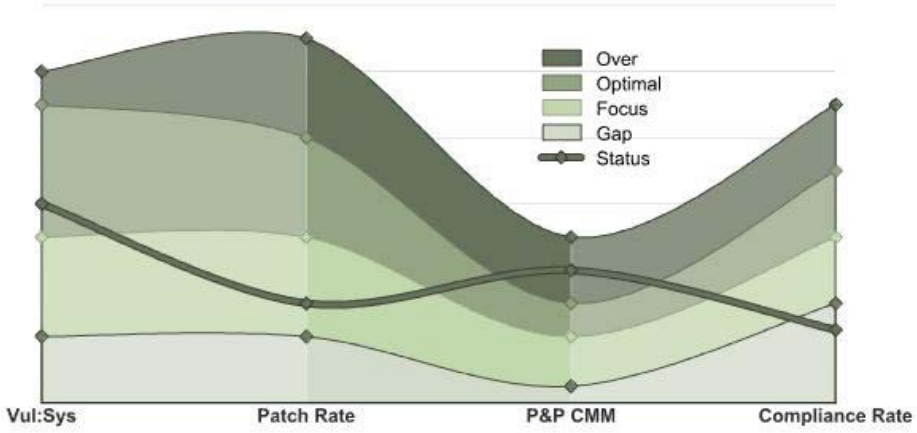


**Figure 3 - Security Services Management**

A simplified example of security services management is demonstrated in Figure 3, which exhibits the characteristics of security by combining people, process and technology elements into each category. Vulnerability to system ratio – technology - is based on the role and status of a given system. This can be aligned to business unit or specific service. Patch rate – technology and process - is defined by the risk of an identified vulnerability to a given system role. The capability and maturity of people and the processes they follow are evaluated. Compliance rate may represent the status of combined actions, such as implemented controls and validation of those controls.

The delta in status level is related to the dynamics of a given area or the rate of potential change. For example, the ability to control vulnerabilities relates directly to their unpredictability; therefore, what constitutes a level of capability needs to be sensitive to the dynamics of that control area. In contrast, the level of maturity of processes is less prone to short-term change and consequently has a limited spectrum for ranking.

A common infrastructure provides the missing ingredient in offering security management. Similarities exist in traditional network-related services; their creation, provisioning, changes, and performance are all governed by service level agreements and network-related capabilities. When a security thread is introduced, security itself becomes another network-enabled service that can be deployed and managed based on specific needs aligned to business objectives. Therefore, the same metric strategy used to govern IT services provided by the existence of a synergistic network infrastructure can be readily applied to security services management.

As with IT services, which are founded on the ability of technical attributes that offer broad capabilities, Cisco's approach is representative of bringing that same service-oriented predictability and scope to information security. This advantage cannot be understated. The evolution of adoption to acquire the

security thread will eventually be the foundation for managing security in measurable business terms in addition to increasing the security capability of the organization.

## Philosophical Challenges

Point solutions have reigned supreme in the light of information security. This is the result of two distinct and aging conclusions. On one hand, the availability of a comprehensive security suite that offers the advantages of realizing a security thread throughout the infrastructure, and all that it implies, simply doesn't exist. On the other hand, using a point product that meets your specific needs – at that layer – is the most effective approach.

As demonstrated, these are not forgone conclusions. Introduced earlier, Cisco's role in the network has provided them with the opportunity to offer a consistent solution, thus yielding the elusive security thread. While for Cisco this is a natural evolution in supporting their customer demands, people are confronted with the two legacy conclusions.

Early in the evolution of technology there was a saying, "You would never be fired for buying IBM." As point solutions developed, companies saw an opportunity to separate themselves from constraints associated with a single vendor and obtain greater flexibility. However, the adoption of a standardized platform in the network and even at the operating system level is being seen. Today, Cisco's security solutions are effectively no different from the introduction of new routing protocols or lower layer architectures. The reality is people do not associate broad security capabilities with the network – this could not be further from the truth.

The contentious factor is that many see the network as a utility and its ability to make security decisions is relegated to upper layer solutions and applications. This assumption has led us to employing diverse solutions to manufacture the consistency that a network can and does provide. We accept sophisticated logic in the network fabric for quality of service, routing, protocol manipulation, performance, availability, and service support. These capabilities are possible in some instances because the network devices are exposed to every detail of the transmission.

One of the more prevalent arguments against the network's viability in security has to do with worms and application diversity. For example, worms propagate in a number of ways using methods to avoid detection. Additionally, they may interact deep within application communications making it very difficult to detect at the network layer. Similarly, applications may provide services utilizing multiple protocols and ports, making it nearly impossible for the network to differentiate what is good from bad. However, the role the network plays does not require only these direct capabilities. It is about establishing and enforcing policies, gaining visibility, and providing the ability to confidently make broad changes to the environment in a proactive manner. For example, if a new worm is identified, the network will permit the investigation of remote systems to ensure they have applied the latest signatures prior to allowing access, and if not applied it can provide a dedicated segment for isolation and evaluation. Moreover, if the communication characteristics of the threat are known, administrators can quickly implement controls throughout the environment, reducing exposure to attack or proliferation. Once implemented, the added benefit of automation of key security processes can occur.

## Summary

The perception of the network and its role in security is changing dramatically. The network is not about the processing of information at the network level anymore, as exemplified in traditional thinking. It is the use of an intelligent network as a system to thwart infection, implement proactive changes, and obtain the much

needed visibility and management of the state of controls. It is taking advantage of an infrastructure in a new approach that utilizes it for what it really can accomplish.

As stated above, the network touches everything and it is in the perfect position to permit or deny communication, manage expectations for participation, and act as an informed gatekeeper to resources. Hackers, malware, spam, worms, and a plethora of other undesirables have used the network as an enabler. The impacts from these threats materialize in upper layer entities, such as collaboration systems, financial systems, storage systems, and applications, drawing our attention away from the very thing that can be used to gain control.

Enforcing policies and ensuring those policies are in alignment with business objectives and demands have remained the responsibility of people and the processes they follow. It has been proven over and over again, either by the continual suffocation of business by attacks or by the endless battle to determine the condition of the security posture, that current practices are not as effective as they need to be. As a community, the network has not been fully leveraged in the realm of security. The network has remained a silent, but highly capable member of the business.

Security is realized by a few important and distinct abilities. Knowledge about the condition of controls, their effectiveness, and adherence to set policies is essential to maintaining a proactive stance, not simply a defensive or reactive posture. Having confidence in making changes to the environment and understanding the relationship of those changes to business processes and the level of risk is paramount to an effective security program. An intelligent network provides these fundamental needs and can exceed business expectations for security and compliance by offering features supported by these core attributes.

With a security-aware network you gain unprecedented control, clear visibility, and enhanced management. Empowered with these basic attributes, companies can expand services with confidence, reduce exposure to unwanted threats, meet emerging regulations more effectively, gain investment predictability, and align security efforts to the demands of the business.

Until Cisco's emergence as the first to challenge the perceived role of the network in providing the elusive benefits of security, companies have been fighting the battle between compliance and vulnerability with only two of the three tools at their disposal: people and process. Cisco's approach in making network technology a formidable member of the security posture is undeniable. The role of the network in protecting the business will never be the same.

## Conclusion

In the face of sophisticated threats, numerous vulnerabilities, and regulatory demands, companies are challenged to find a solution that can provide meaningful protection and compliance while remaining sensitive to corporate dynamics and investment constraints. While the most recent focus has been at the application layer, it is the network that will emerge to support the alignment of business and security. Networks are everywhere; they are the means of business enablement and are the frontline of controlling communications. Security threats and the havoc they cause are the bane of corporate effectiveness. However, their very existence is possible because of the network. The network can enhance security, not by digging deeper, but by providing the platform for consistent controls and employing those controls comprehensively.

The long-term affects of a common security infrastructure are many and with it comes the ability to manage security as a service to the business and demonstrate its role in broader corporate objectives.

Finally, companies can have assurance in making investments in the network because the network is a constant and integral part of business. As the foundation, it is quickly emerging as a security-enabling component to address current and future challenges.

At the most basic level, security is the ability to understand the state of the environment, enforce controls, and have the confidence and capability to enact decisive changes. The role of the network is beginning to change, taking on a new role in supporting information security objectives. Networks are quickly becoming the enabler for organizations to address security threats and vulnerabilities, regulatory compliance, and even business demands.

## About INS

International Network Services (INS) provides network consulting services and business solutions to help companies build, secure, and manage business-critical network infrastructures. Our end-to-end network consulting solutions address customers' needs in Next Generation Networking, Security, and Network & Systems Management, helping them optimize their business to better face competitive challenges and meet future demands. We are one of the world's largest independent network consulting and security services providers with a track record of thousands of successful engagements. INS is headquartered in Santa Clara, Calif., and has offices across the U.S. and Europe. For additional information, please contact INS at 1-888-767-2788 in the U.S., 44 (0) 1628 503000 in Europe, or 1-408-330-2700 worldwide, or visit www.ins.com.