

**INTRUSION TO INTEGRITY:  
PUTTING PRODUCTIVITY BACK INTO  
THE NETWORK**

**AN ECONOMIC APPRAISAL SPONSORED BY  
CAPTUS NETWORKS, INC.**

**OCTOBER 2003**



**ABSTRACT**

Frontline managers of networks today can attest to the fact that security has quickly outpaced their expectations in terms of budget capacity and forced a significantly harsh effect upon labor resources. More clearly, the battle has become a see-saw motion of investment in security technology while attempting to balance the needs of network reliability. Signature-based intrusion prevention systems (IPS) remain under the constant duress of keeping up with attack forensics and trying to outsmart the next dynamic denial of service (DDoS) assault. Arguably, this approach to preemptive safeguarding against hacker activity presents a no-win situation for organizations in search of placing spending limits on security while ensuring adequate protection of their business applications.



**SECURITY  
SPENDING  
HAS RISEN  
ON AVERAGE**

**18.4% IN  
2002, AND  
THIS FIGURE  
COULD  
EASILY TOP  
24.3% FOR  
2003**

While security appears to be everyone’s concern, policy and rules for network operations can now be applied intelligently across the board with a level of automation that curbs the drain of IT resources. Our research has shown that the compound annual growth rate (CAGR) of costs associated with security spending has risen on average 18.4% in 2002, and this figure could easily top 24.7% for 2003, with all other factors held constant. This means that the cost centers weighed against security functions have escalated to an amount *nearly double* than was previously seen two years ago. Moreover, the manual labor contingency required to apply security continues to hold the enterprise hostage with an average CAGR increase of 31.7% for labor inputs alone. And looking deeper at the division of tasks ascribed to network administration, we see these data supported by a surge in focus of personnel attention on security matters versus normal provisioning assignments—at a steep ratio of 3:1. This establishes a strong business case for seeking a path of network availability that requires less manual intervention and a higher degree of intelligent automation.

Matched by increased concern that security may just rail the next IT budget sinkhole, the challenge of the network domain at large is to connect the issues of transport availability and security together. Combining these two elements, network availability and security, has evolved to proliferate a radically different view of how productivity and protection converge. Labeled as *network integrity*, the term itself affirms credence to the importance of business productivity and treatment of risks associated with intrusion. In this economic appraisal, we lay forth the various dimensions at which the integrity of networks have superceded the role of basic intrusion detection systems (IDS) and why the assurance of network availability moves toward a higher value proposition to both end-users and IT organizations alike.



On the edge of studying an apparent connection between policy applications and IT users, we illustrate the behavioral and technical economic lessons at work within the collective enterprise—from the small-to-medium company through the scalable network of remote branch offices. The scope of our research applies real-world data from network environments of nearly all types—corporate LANs, WANs, MANs, and mobile IP configurations. But the essential premise of network integrity’s proposition remains the same: *does network availability and security draw a parallel between business objectives and technology itself?* The answer we believe is a compelling ‘yes’, and the rationale that supports this conclusion is as intriguing as the question taken separately.

In the sections ahead, we take special interest in how interoperable technology spawned the externality, or byproduct, of security and why the management of such has been in conflict with the enterprise ever since networks grew beyond the firewall. And as part of the explanation, we unveil some of the key statistical evidence and metrics that define how dramatic shifts in network efficiency play a critical role in business survival.

#### GETTING BEYOND SECURITY MYOPIA

Trends toward applying security services and solutions in recent times have focused on a proactive thwart of attacks by means of prevention and signature-defined network traffic patterns that signal intrusion. Or as the anti-virus realm operates, message headers and packets are scrutinized under a reference dictionary of known agents and code-level variants that have been previously catalogued as digital templates. By early 2001, corporate computing saw some of the worst effects of hacker activity when denial-of-service (DoS) attacks nearly leveled Internet infrastructure. The resulting fix was to proactively erect firewalls of greater strength, implement server contingency plans, and invest heavily in virtual private networks (VPNs) while conquering a never-ending defense strategy. It seemed as though the basis of network security became attached to a negative sinkhole or cost center within the CIO’s budgeting process. A consensus of valuable IT projects were stymied or cancelled outright until security—or a respectful notion thereof—could be verifiably put in place to protect existing information assets.

Aside from the business paralysis imposed by service interruption, organizations became consciously aware of their vulnerabilities and naturally responded by reeling in the control arm through onerous security policy. The question was no longer *if* attack would happen, but rather *when* such attacks would strike. After billions of dollars spent, the nuisance of security is still a pest to the majority of CIOs embattled by shrinking budgets and a heightened awareness of technology’s luster in delivering business value. Justification to dilute even more resources proves to be fought with cynicism and negative emotion; security continues to bear the brunt of swelling budget attrition for otherwise important projects.

#### ECONOMIC IMPLICATIONS OF NETWORK INTEGRITY\*

- *A Heavy Workload for Security: 3:1 ratio of security tasks versus provisioning tasks*
- *Network Disruptions on the Rise: 41.6% Increase Since 2000*
- *The Ransom: 31.7% annual growth spend for security labor*

\*Source: Modeled from extracted data of the “Network Economics Study”, OMNI Consulting Group LLP



Stepping away from security’s traditional positioning, we recognize historically that the role of mitigation from risk—whether it implies physical breach or a network breach—has satisfied a path of improvement for business processes and contingency planning. As an example, utility companies protect their power generation assets from malicious harm but simultaneously use their security infrastructure to monitor bottlenecks in the delivery of energy products to legitimate customers. The same can be said for the safety function of risk mitigation within a manufacturing plant; avoiding harm and resource pitfalls imparts sustainable business operations. Both examples give evidence to the fact that security can indeed deliver a secondary range of benefits, or economic enhancements, to the overall value of a firm. So, why the sudden negative perception toward investments in network security as being viewed a necessary evil? In reality, it is more about productivity than a simple risk shelter.

**THE  
QUESTION  
WAS NO  
LONGER IF**

**SECURITY DELIVERS A COMPLEMENTARY FUNCTION**

**ATTACK  
WOULD  
HAPPEN,  
BUT RATHER  
WHEN**

Consider the following: *if your network was down for any given amount of time, what impact would this have on your customers, employees, or suppliers?* Chances are, the instance of a network outage says that some amount of business connection is lost and productivity is slowed either directly or indirectly. Consequentially, customers that can’t place orders translate to a direct loss of revenue; employees impaired by a network glitch means an indirect breakdown of communication capacity. Some operations can live for days without the network functioning properly; others may be forced into catastrophic situations. Therefore, the bottom-line message of network availability is an important one, especially given the reliance on network throughput both internally and externally.

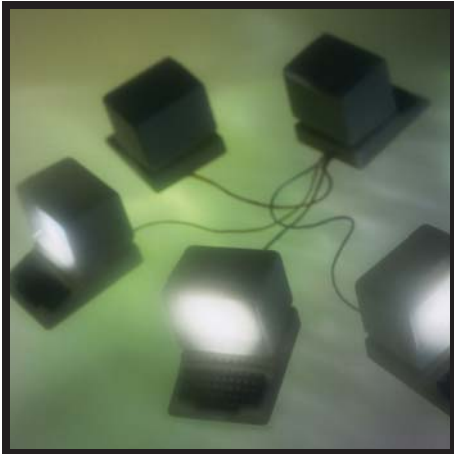
**SUCH  
ATTACKS  
WOULD  
STRIKE**

Accepted that continuity of business operations is most important, then why is network security not an integral component of assuring the productivity of customers and employees? After all, a firm that stays productive (through no fault of its own) has an opportunity to deliver a basket of goods and services of market value for an economic profit. This marks a business priority above all else, and security becomes one of the inputs that allows production to occur without interruption. Just as electricity is needed to power computers and the cash register, so is the necessity of security to maintain availability of network infrastructure that carries value to the enterprise.

From an economic angle, we say that security can be classified as a *complementary* product of network availability—meaning that security complements, or enhances, the value effects of a continuous network environment. Complementary products strengthen the essential service by supporting one or more of the value structures in such a way as deemed important to its overall configuration. Quality of service (QoS) features may also be labeled as complementary to network availability since these enhance the overall of utility of a connected network. Without security, network intrusion may occur and hence availability of service is compromised



or becomes null. Service level agreements (SLAs) may fail to be achieved while assurance is left to the wayside. And although complementary services such as security may operate independently of one another, the underscored lesson is that some core products can not operate effectively



without their complementary attributes. By far, security is one of those staple components that is necessary to assure network availability, but is often disguised under a separate and detached technology label.

**MINIMIZE COMPLEXITY TO  
MAXIMIZE BUSINESS PRODUCTIVITY**

Technology in the past decade has subtly changed the level of computing automation and users seeking simplicity—enabling applications and people to operate without much technical intervention.

Rather, networks, by themselves, erupted into a hierarchical set of oversight divisions—administration, provisioning, performance monitoring, and auditing in no particular order. The foregone conclusion in the midst of complexity is to assign an engineering function to every detail regarding the user’s interaction with the network. Notwithstanding its own silo, security routinely falls into the bucket of network administration and adds significantly to the load factor of tasks assigned to IT personnel.

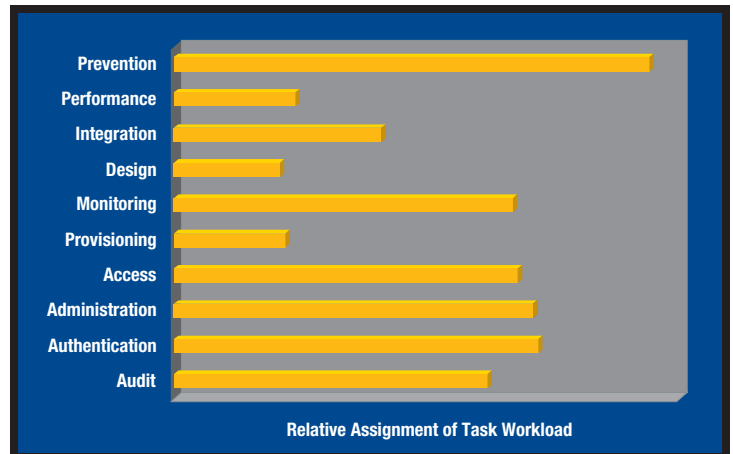
Our research of more than 4,000 organizations worldwide and their behavior respective to network utility shows considerable room for improvement when it comes to allocation of resources assigned to the tasks of network security. For the period of 2001 through the second quarter of 2003, we said that the task of network security displaced basic provisioning functions by a whole number ratio of 3:1. That means, for every single network engineering task associated with provisioning activities, nearly three tasks can be ascribed to audit, authentication, access, and security functions. And by any indication of today’s trends, the complexity of network users appears to be climbing as encryption and mobility come to the foreground of concerns plaguing network engineers today.

But complexity itself is not a solo anchor that drags engineering departments. User interactions through external service providers and the everyday business environment feel this burden at the core of disruption, in fact somewhat unequally. Viruses and the latest mutants of infection multiply within computing groups as a result of user collaboration. Vulnerability and risk of intrusion lie, to a greater extent, with those individuals that fail to adhere to security practices in general. With rare exception, it is most always the non-IT employee or external customer who suffers from the fracture of a broken network and the adverse reaction to a highly complex IT environment. An unavailable network, despite the blame of negligence or error, is a dysfunctional asset to any organization.

THE GOAL OF  
EVERY FIRM  
SHOULD BE  
TO MINIMIZE  
THE DOWN-  
TIME OF  
INFORMATION  
TECHNOLOGY  
AND SEEK  
TO MAXIMIZE  
ITS OUTPUT



Certainly, the goal of every firm should be to minimize the downtime of information technology and seek to maximize its output of core goods or services to its customers. The takeaway example from the maturity of network structures over the years is to make *simplicity* a competency of every major directional initiative. Simple, monolithic platforms win over the one-to-one patchwork quilt of individual protection, and even more so when dealing with security as an overarching shield. By freeing IT personnel to focus on capacity planning and implementation projects, the guesswork often associated with making security seamless displaces yet one more burden from technology's complexity.



Resource Allocation Priority within Network Computing

*Technical Efficiency*

As we stated before, every company should view their operation as an economic production function, which is essentially a set of inputs (e.g. land, labor, and capital) that are applied to produce an output (e.g. goods and services). On the left side of the equation, the inputs are assembled in such a way as to minimize cost and maximize productivity, or sometimes profit. Technology is one of the staple inputs for most businesses today, and by adding certain levels of network technology to the production function, we see costs incrementally decrease and may observe a rise in productivity as an output. Whenever a firm moves closer to optimizing their available inputs and outputs because of technology, we say that *technical efficiency* is present to induce this change.

Network availability and intrusion protection are no exception to familiar technology inputs. These elements raise the technical efficiency quotient by assuring transport connections and minimizing disruptive threats to the productivity of an organization's computing environment. And when removed from the equation, statistical evidence points to a 41.6% rise in disruptions that take place in the course of everyday network traffic. That translates to a cascading frequency of absent production capacity that could otherwise be applied to producing economic profits. In fact, many North American firms saw the greatest change in connectivity outages during the boom era of early 2000 when the business climate was operating at peak gross domestic product (GDP) levels. It remains somewhat less obvious, however, that the rise in disruption was statistically connected to higher levels of interconnectivity. Thus, applying an intelligent, automated approach to network integrity is one move closer to a direct return on investment of technology inputs.

STATISTICAL  
EVIDENCE  
POINTS TO  
A 41.6%  
RISE IN  
DISRUPTIONS  
THAT TAKE  
PLACE IN  
THE COURSE  
OF EVERYDAY  
NETWORK  
TRAFFIC

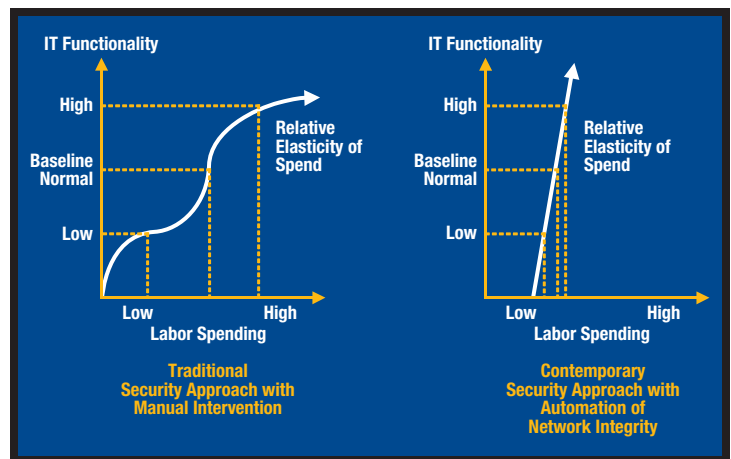


*Operational Efficiency*

Separately from the addition of technology inputs in the production mix, our research pays close attention to the effects of labor on changing the productivity curve and how networks survived (or failed) through the rash of hacker intrusions over an observed period of three years. Because the assignment of inputs and production output is a deterministic factor, *operational efficiency* looks at the configuration of these variables and examines the optimization of labor requirements. A given arrangement of labor resources will undoubtedly produce a host of different output choices; the majority of business decisions involve resource allocation to achieve a preferred outcome.

Inside the network architecture, an influx of attacks and unpredictable bandwidth patterns has left global business ill prepared to apply the necessary labor resources to combat an uncertain problem. Scrambling to stay ahead of the next interruption is a game that few seldom win because the infinite possibilities of service disruption far outnumber the resources required to predict and protect. Even the most proactive vanguard of virus vendors can hardly keep up with the inflow of newly identified strains and patterns of network forensics. So, the solution must be one that reduces the apportionment of labor dedicated to the task and allocation of those resources to areas of better productivity.

In our study of network behavior, we found that organizations typically increased their nominal economic spend for internal and outsourced labor to solve security functions by an amount equal to 31.7% year-over-year since 2001. As pointed out earlier, this highlights a concern that labor is an increasingly significant line item in the assurance of network availability and how technical resources may be consumed in multiplying proportions. Also, the corollary to greater spending on technical labor is a nominal reduction in economic profit or productivity gains.



*Neoclassical Economics of IT Functions and Elasticity of Labor Spending*

*Note: A comparison of labor spending and the relationship to IT functionality; automation of security versus labor intervention\**

\*Source:  
OMNI Consulting Group LLP



## NETWORK INTEGRITY: A MODE OF STATISTICAL RELATIONSHIP

Thus far, we discussed how the synergistic blend of network availability and the function of security can be mutually compatible by lowering complexity and increasing productivity. Taken separately, these two functions have held differing opinions of their value with respect to the overall support of network performance. But more so, the endgame is about a network that functions to serve its users effectively and with a certain degree of predictable reliability.

THE  
ENDGAME IS  
ABOUT A  
NETWORK  
THAT  
FUNCTIONS  
TO SERVE  
ITS USERS  
EFFECTIVELY

Jack Quinnell, vice president of product management at Captus Networks, Inc., cites the difference between network availability and the role of security as a catalyst for convergence—a confluence of terminology best summed up as *network integrity*. A network with high availability probably would not exist for long if granted a permeable layer that lacks security. Nor would a highly secure network be of much use if the availability of transport protocol was absent or missing in pieces. From that perspective, both pieces are integral in order to allow an optimal network infrastructure to perform at its best and provide direct service assurance.



Network integrity enhances this view by incorporating a level of *predictability* with regard to intelligently configuring traffic loads and scouring packets for threat anomalies as the flow passes into and from the network. To accomplish this feat, statistical sampling and predictive analysis dynamically adjusts traffic to routing conditions and simultaneous extraction of threats that match atypical patterns. Reliance on detection lists only comes so far in thwarting attack; the plague of DDoS attacks may best be eliminated by analyzing suspicious traffic patterns in real-time versus after the conflict.

Future avoidance strategies that mitigate the risk of attack by method of real-time sensing will embrace prediction at the core. And while hacker penetration and the frailty of networks stand to be tested even further, it seems logical to conclude that algorithmic programming and statistical sampling work to assist the automation cause of managing the threat envelope. Consider the next wave of detection—and protection, for that matter—as a mode of sensory capability guidance by statistical intuition.



*Intrusion as a Byproduct*

The more we learn about intrusions, whether it be through the aftermath of an attack or the discovery of new access pitfalls, the better we are able to cope with these events as a byproduct of interconnectivity and hence safeguard ourselves from network outages. Thinking of intrusions as an *externality*, or a consequence of open network environments, presents an opportunity to predict how applications and business processes respond to threats. In a similar context, the benefits of open commerce bear the price of theft by direct or indirect attack, yet commerce still continues to operate beyond the risk of theft. Likewise, we can predict that intrusion will always be a consequence of open network interoperability but may be sharply curtailed—if not contained—by assuring performance against the landslide of conditions under which attack might occur.

AN  
INSURANCE  
POLICY  
AGAINST  
RISK OF  
LOSS IS  
ONLY USEFUL  
AFTER  
FAILURE  
OCCURS

**SHAPING UP FOR THE SAKE OF CONTINUITY**

The puzzle of network security is no longer about hacker penetration or malicious behavior. Rather, the departure from past thinking is prompted by an obsession with making the network perform optimally, at its best and all the time. Service providers know this issue firsthand: *keep the network running or risk losing the customer*. Lose the customer, and the reason to stay in business is certainly a disastrous fate. But the attention of many firms and service providers has been derailed by fear and the hedge of risk in the event of an attack. The preferred business logic of choice is, of course, making the network prevent disruption through intelligent automation.

While every organization should direct their attention to economic improvement, seeking the advantages of assured networks will find higher value returns on their overall technology investments. Keep in mind, productivity wins over disruption, and security is only purposeful if it is applied consistently across the enterprise. An insurance policy against the risk of loss is only useful after failure occurs.

Accepting that the parallel between network availability and achieving business value exists, our research shows a direct correlation between the return on investment of network integrity and management goals. Shareholders demand profit performance while employees, customers, and suppliers demand a reliable connection. When the network falls down, so does the business objective. And placing security in the context of why network performance is critical may be the next step that moves companies to overhaul their computing strategy. Either way, business continuity is shaping up to be what matters most in every decision.



**PART II: YANKEE GROUP**

From data traffic to voice over IP communications, the impact of network integrity systems (NIS) is gaining speed in the vendor community. As part of a special report on security solutions and services, The Yankee Group (Boston, MA), authored an accompanying report as a primer for understanding the technical roadmap of NIS within the extended enterprise. The thrust of their work serves as a defining edge in the marketplace positioning of network innovation and how vendors align themselves by capability in handling the network integrity premise. A copy of the report may be secured by visiting [www.captusnetworks.com/yankee](http://www.captusnetworks.com/yankee).

**CURRENT**

**DATA**

**INDICATES A**

**31.7%**

**ANNUAL**

**GROWTH**

**SPEND FOR**

**SECURITY**

**LABOR**

**METHODOLOGY ENDNOTE**

Conclusions and various perspectives contained within this report incorporate the latest economic data pertinent to the network operations of diverse organizations around the world—spanning the domestic U.S. and European commercial enterprise. Our sample population (n=4,127 companies) was queried from a previous data repository entitled, “Network Economics Study (1999-2003)”, whereby we collected through primary research methods information regarding companies and individuals with respect to network computing behavior. Beginning with the compilation of these data concerning network economics and security utility, the initial task involved applying multivariate analyses for logistic regression and chi-squared automatic interactive detection (CHAID) relationships. We expanded our modeling exercises to concentrate an understanding of the relationship between business output and the role of security functions.



#### ABOUT CAPTUS NETWORKS, INC.



Captus Networks Corp. provides comprehensive intrusion prevention security solutions for enterprises, ISP's, government agencies and universities that need to ensure predictable network availability while minimizing operating costs. The company's unique business-driven, policy-based security approach automatically preempts all types of unwanted network behavior. Captus is privately held and headquartered in Woodland, California. For more information visit [www.captusnetworks.com](http://www.captusnetworks.com) or call (877) 9-CAPTUS.

#### ABOUT OMNI CONSULTING GROUP LLP



Founded in 1989, OMNI Consulting Group LLP is the premiere source for empirical knowledge behind today's fast moving technology marketplace. With an impressive global network of economists and research practitioners, the firm serves many of the world's largest technology organizations and offers an unbiased approach of quantitative standards to address client-focused initiatives. OMNI Consulting Group fosters the understanding of market dynamics through an application of econometric solutions in a wide array of advisory and management research functions. Practice units within the firm concentrate on merger and acquisition support, technology audit and assurance, and intellectual asset valuation.

No longer is market blindness an excuse, but rather an opportunity to witness the next horizon. Discover the insight of technology economics at [www.omniconsultinggroup.com](http://www.omniconsultinggroup.com) or call (530) 750-5199.

#### ABOUT THE AUTHOR

Frank J. Bernhard is a technology economist and the managing principal of the Supply Chain and Telecommunications practice at OMNI Consulting Group LLP in Davis, California. His research focuses on emerging knowledge technologies and the econometric models that explain market phenomena in the past decade.

Regarded as a pioneer in the subject of technology economics, his writing appears across many different industry and trade media sources, including *Intelligent Enterprise*, *Red Herring*, *Telephony*, *Technology Investor*, and the *Wall Street Journal*. He may be reached at (530) 750-5199 or via email at [fbernhard@ocg-us.com](mailto:fbernhard@ocg-us.com).





vision  
beyond  
technology

© 2003 OMNI Consulting Group LLP. All rights reserved.

OMNI Consulting Group LLP, Davis, CA 95616

Tel: 530.750.5199, Fax: 530.750.3710, Email: [information@ocg-us.com](mailto:information@ocg-us.com), Online: [www.omniconsultinggroup.com](http://www.omniconsultinggroup.com)

*Captus Networks, the Captus Networks logo, and all product references to the company are trademarks of Captus Networks, Inc. Other brand and product names are trademarks of their respective holders. All specifications are subject to change without notice. All opinions, factual notes, estimates, and statistical references constitute our judgment as of this publication date and remain subject to change without notice. This economic appraisal may not be duplicated, reproduced, or retransmitted in whole or in part without the express permission of OMNI Consulting Group LLP.*