



Mitigating Economic Risk Through Security Technology:

An Appraisal of
WatchGuard Technologies, Inc.



October 2002



Abstract

Appearing daily across the headlines of major newspapers and periodicals, global security has moved to the forefront on business concern. And the economic losses ascribed to such attacks and breaches totals a staggering sum in billions of dollars (US) annually for companies spanning the continents. For businesses of electronic commerce and highly concentrated information architectures, these disruption figures soar even higher than traditional manufacturing and service sectors. Yet, the data encapsulated in our ongoing study of network economics on a worldwide basis point toward an ever-increasing frequency of activism and tangible asset destruction as direct consequence of improperly protected organizations. We commenced observation of several multifaceted categories of behavior and measurement for network operations in early 1999, and today, continue to monitor the sampled population for change as trends evolve in network computing behaviors.

This report—as an economic appraisal of network security attacks and vulnerability to digital intrusion—sets forth to define components of risk mitigation through the investment in firewall appliances and server-side preservation technologies. Aside from descriptive statistics that illuminate real-world occurrences, the numerical values contained herein can be applied to nearly every organization seeking to lower their economic risk associated with information technology compromise and justify nominal expenditures for securing their assets. Security can no longer be regarded as an auxiliary technology investment, but rather as a core investment in the capitalization of the enterprise business model—alongside the host of other inputs that ensure business output and productivity.

The latter sections of the appraisal present an overview of Risk Mitigation Measurement (RMM) and how organizations can approach such methods as policy-based network security functions and Virtual Private Networks (VPNs) to quantify elements of their economic risk position. Throughout the underlying subject matter, we offer an explanation of the behavioral and historical economic evidence that continues to plague the integrity and success of business operations from a security vantage.

Security as a Risk Mitigation Strategy

Risk begins with a perceived vulnerability and the acceptance of safeguard methods to reduce the likelihood of a negative or undesired outcome. In the economic sense, risk is largely concerned with probability of such adverse outcomes and what factors contribute positively to produce such an event. To an IT manager, risk might mean the chance or frequency of disruption in the network environment—intentionally or unintentionally. Still, the subject of risk cannot be ignored from a contingency planning or information asset

point of view. Staying within the purview of the IT and network realm, risk imparts a need for attention in three distinct areas: *definition*, *measurement* and *mitigation*.

Definition of risk precedes any other component because it starts with setting boundaries—or zones—that determine the scope and outcome of any undesired outcome. For instance, not having a firewall in place for your Internet gateway allows free roaming of public users within the four walls of your business. Risk inviting? Absolutely. A host of undesirable outcomes can unfold and inflict significant harm among your employees and their productivity. But what about setting scope and boundaries? Internet access may only be limited to a specific server, or external gateway, in which case damage is restricted to a concise section of your IT environment.

Limits—and the ability to define zones of impact—are of primary importance in the process of defining risk and its total impact on the organization. These limits, with regard to network operations, have been analyzed and studied as linear functions to ascertain different types of exposure and their relative probability of negative outcome. In other words, setting limits on the type of user (e.g. wired network versus wireless) can allow us to set the boundaries for assigning criteria to the risk equation. While most everything can be measured, few tasks are more difficult than establishing the actual definition of risk as an inventory of impacted resources and outcome probabilities.

Next, with our definition of risk in hand, we move to understand how to *measure* risk itself. Since risk is comprised of negative outcomes and their assigned probabilities, it is best to start the measurement process by taking an inventory of the various types of outcome that may occur and with what frequency they can be observed. During the course of studying a wide breadth of organizations and their network operations, several dominant risk outcomes clustered themselves in the following categories:

- a) **Internal Disruption**—the compromise of network assets as a result of unauthorized or intentional intrusion from a firm's employee or validated user
- b) **Passive Code-Level Intrusion**—the introduction of software agents or script code to the network environment (e.g. worms, viruses, etc.)
- c) **External Disruption**—the intentional and manual process of network or information disruption by an outside system or individual (e.g. network hackers, denial of service interruption, etc.)
- d) **Authentication Forgery**—the use of forged identity credentials to gain access to information assets or systems without authorization
- e) **Extraction**—the intentional or unintentional export or deletion of information assets without authorization

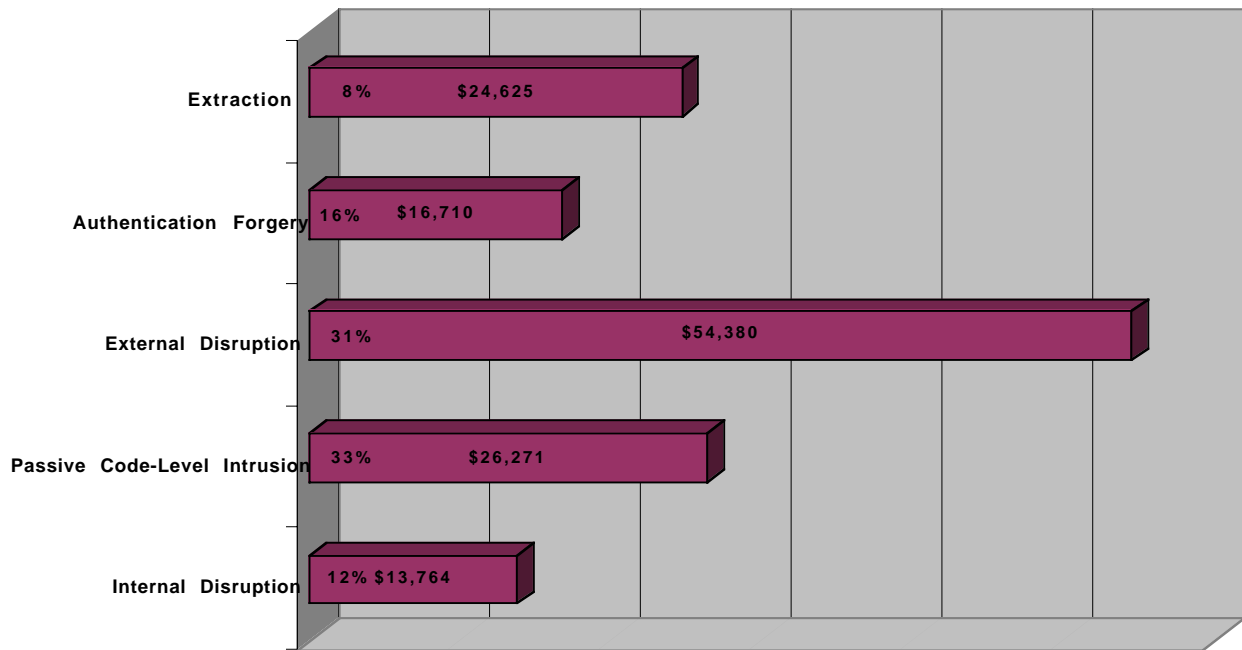
Looking at each of these risk categories, we can look at the data and make two additional determinations regarding frequency (as a probability) and the extent of each in terms of damage (magnitude of loss). In Figure 1.1, a list of these categories is given alongside the corresponding range of frequencies and the measured average value of

loss (in whole US dollars) associated with these activities. Keeping in mind that these data were collected across organizations of disparate sizes (from small businesses to large enterprises), the order of scale in terms of frequency and size of loss for your particular organization may be higher or lower, depending upon several key factors. In our assessment of these elements affecting network vulnerability, we applied statistical patterns produced by Factor Analysis to determine positive correlation among the following variables:

- a) **Employee Density**—the number of employees within an organization
- b) **Branch Locations**—the number of branch facilities or locations outside of the parent headquarters
- c) **Type of Operations**—the primary nature of business products and services, ranging from the production of low-skilled consumer goods to complex intellectual services
- d) **Employee Mobility**—the ability and capacity for employees to access network services outside of a wired LAN environment
- e) **Average Employee Earnings**—the threshold dollar amounts paid to employees as compensation for labor earnings
- f) **Annual Gross Revenue Product (AGRP)**—the amount, adjusted in US dollars, of an organization's earnings or intake of capital proceeds

Figure 1.1 Dominant Risk Outcomes

Shown here with relative percentage of frequency and average loss value per incident



Economists and statisticians alike use the method of Factor Analysis to boil down the most important variables of any measurement equation so as to assess their interaction with each other and determine relationships. For network security purposes, the above-listed variables proved to be the key factors associated with risk of loss and measuring the loss proportions in differing organizations. It is important to remember that the frequency of loss varies according to the relative change of other variables, and likewise the magnitude changes according to the same.

The end game, however, is wrapped inside the *mitigation* process and how we abate risk by lowering our odds of such predictable negative outcomes. Traditional insurance companies, and even those insuring losses in the digital property space, rely upon actuarial figures and statistics to determine a premium for an insurance policy—to hedge against the risk of loss based upon known criterion. In computing the premium, the information regarding the policyholder's risk environment is scored and then aligned to a premium rate structure. Again, based on known factors such as those in Figure 1.1, we can begin to look at technologies that lower our risk of exposure to malicious attacks and disruption of information assets—forcing a significant reduction in the probability of facing such negative circumstances. And by analyzing your organization's risk position in contrast to its relative bearing for loss, the value proposition becomes one of economic sensibility in exchange of dollars spent for mitigation of risk associated with the undesired effects.

According to our observations of these data, for each dollar spent toward a security investment model, companies can lower their risk quotient by an amount equal to a multiplier of 33.4. For example, this means that an organization spending \$10,000 (USD) on network security investment can effectively lower exposure to losses associated with network risk by an amount equal to or greater than \$334,000 (USD). Considering that the average organization places 5.97% of their annual gross revenue product (AGRP) at risk without provisions for contemporary class network security in place, the investment model for network security begins to take shape in the premium paid to mitigate loss. And loss is inevitable without the appropriate defense in place—as only time and probability can tell.

Technology Contrast: A Case for Economic Investment

A number of firewall technology vendors produce solutions focused upon protecting individual users and the IT environment at large from the thwart of hacker penetration and malicious attack—risks that ultimately disrupt business operations and impose considerable costs of recovery. WatchGuard® Technologies, Inc. engaged us to examine the broad base of network economics and breach using available macro level study data while comparing the capabilities and feature sets of their products developed toward reducing risk. In looking at their technology offering as a composite of risk mitigation

**“One
dollar
effectively
lowers
your risk
by 33.4
times the
invest-
ment”**

and network enhancement benefits, the referendum for an investment decision is one that goes much deeper than a simple ROI (return on investment) calculation—rather it supports a wide value chain.

And to get a firm grasp on these value chain constituents, we apply an economic method or theory known as Economic Value Creation—or simply, EVC for short. The notion of EVC imparts summing together each of fundamental areas in which a technology, or group of technologies, adds value to the efficiency equation. Technology, by design, should make business operations more efficient when it displaces or augments a process that enhances productivity or constrains cost. When talking about efficiency, it is important to recognize that the concept implies three different approaches: *technical*, *operational* and *economic*.

Technical efficiency—in the context of firewalls, information asset protection and general network security provisions—relates to the change at which technology alters the risk equation as a direct consequence of the technology additive. Firewalls enhance technical efficiency by reducing the negative byproducts of attack and breach with respect to ensuring the continuation of normal business operations. If the technology was not in place, and an attack or breach was to occur, then business production would be disrupted either directly or indirectly. In any case, the ability of your organization to produce its goods or services at the same rate would be lessened—if not ceased momentarily.

Complementary to technical efficiency advantages, the approach of *operational* efficiency concerns itself with the configuration of capital, infrastructure and the resources necessary to maintain business operations. When support staff burdens themselves with the added labor and resources required in correcting a negative security outcome, this takes away valuable productivity that would otherwise be applied to normal business operations. Technology that aids or preserves resources within the business configuration is said to improve operational efficiency—following the old adage of ‘doing more with less’. Operational efficiency is vital when contemplating the labor input necessary to maintain a network environment, especially from the aspect of supporting end-users and strategic projects that come before recovery operations.

When most technology vendors discuss efficiency, what their message often conveys is that the solution will save money—or more appropriately, minimize costs. But saving money is only a small part of *economic* efficiency when assessing the incremental capacity to minimize capital expenditures or maximize revenue. At face value, technology should conserve at least some resources when selected to replace inefficiency or enhance revenue opportunity. Network security not only protects companies from the costly expenditures associated with cleanup and recovery from attacks, but it can also drive productivity above and beyond normal levels by enabling network assets to perform more effectively. And effective networks translate to bottom line improvement on a real cash basis.

Taking each of these efficiency approaches separately and together, EVC creates

a different picture of the value proposition by addressing the investment from a contemporary angle. Technical efficiency drives companies to mitigate risk by lowering their probability for network violation and allocating their productive resources more diligently. Operational efficiency ensures that the configuration of capital and infrastructure continues to perform as scheduled and that labor resources are best applied to their respective tasks. Economic efficiency drives performance in the financial quadrant and helps companies realize revenue opportunities through reliable networks with predictable Quality of Service (QoS). And measured jointly, the view toward making a business case for network security becomes sharpened across each context.

Data from this study concluded that network security and server-side protection products were the least amount of budgeted expenditure as a ratio of total network operational expense for most companies. All the meanwhile, these same investments in network security generated the highest returns on mitigating loss and ensuring network performance. And from a CIO's perspective, that equates to money well spent in delivering high-value information services to their company.

Firewall Economics: WatchGuard Firebox® III and the Firebox® VClass Advantage

From statistical evidence gathered in our query of firewall usage among companies of all industry classes and sizes, the economic utility is greatest when such technology is applied to the mobile employee class—which is of little surprise since the category of 'Employee Mobility' was one of the chieftain variables that contributed positively as a risk factor. Individuals and systems that access the network outside the permanent walls of a wired company location shelter the largest amount of risk in terms of passive code-level intrusion and extraction of information assets. WatchGuard Technologies produces two variants of complete firewall solutions—the Firebox III and Firebox VClass.

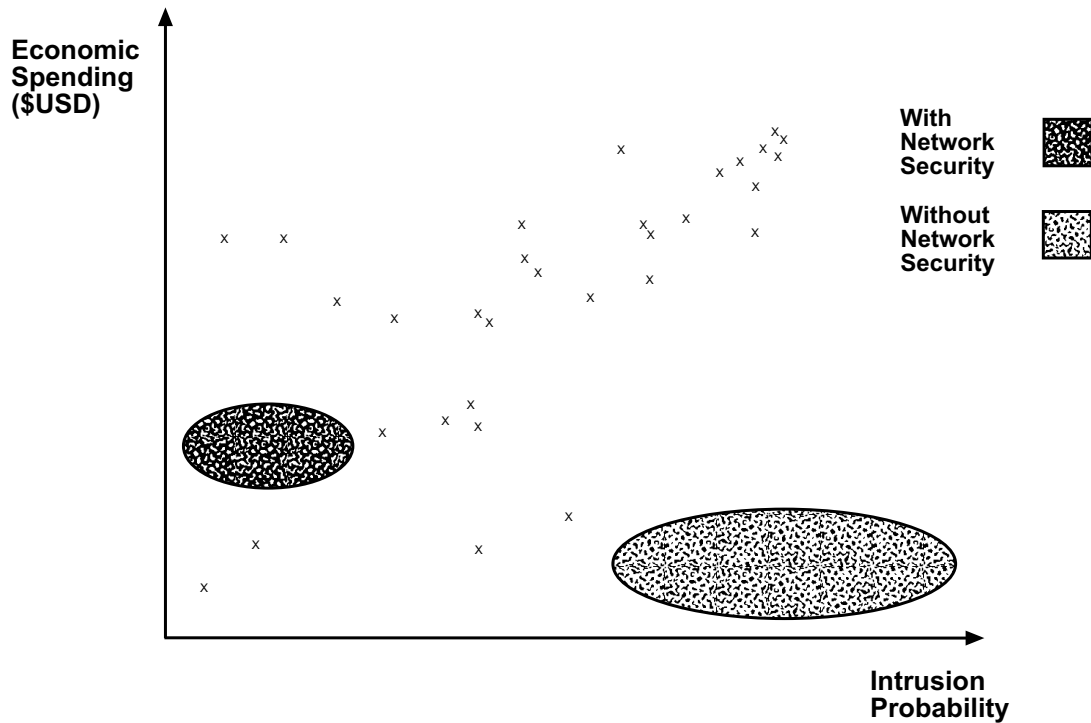
Protection against viruses and worms, alongside malicious attacks from external disruption, can be effectively halted through the use of firewall solutions. Unique to the Firebox III and Firebox VClass, these product solutions offer such features as stateful packet filtering, network address translation and intruder detection resources—translating to a firewall solution that does more than act as an intelligent barrier, but one that lowers the risk factor by control at a single platform. When looking at counteracted network security breaches and trends in a global perspective, firewall solutions accounted for more than 78% of successful first line defenses against attempted intrusion. Lowering risk while spending proportionately to the number of mobile users is critical to maintaining a secure network and effectively minimizing the spread of uncontrolled code-level attacks. Eventually, a well-fortified network of mobile users will strengthen the core performance and protection of digital assets being used across multiple functions of the organization.

In looking at competitors to WatchGuard's Firebox III and Firebox VClass line of

firewall products, other comparative technologies such as Cisco PIX® (Private Internet Exchange), NetScreen™ and SonicWALL™ fail to currently bundle as standard options the same software filtering capabilities for primary defense against code-level intrusion and policy-based packet detection. WatchGuard's competitive edge from a cost of ownership position is firmly grounded in providing a turnkey solution that not only performs the essential firmware appliance functions, but also completes the security loop with anti-virus and sophisticated authentication features. Firewall solutions must look at the total envelope of security functionality and not leave loopholes for optional intrusion points.

Figure 1.2 Economic Spending Versus Intrusion Probability

Shown here in this Cluster Analysis is the relative impact of economic spending in contrast to the probability of intrusion. Note the proportionate scale of economic spending and sharply reduced intrusion probability associated with firewall and server-side protection.



VPN Propagation

Since 2000, VPN gateways continue to grow at steady rates of 27% (2000) and 31% (2001) since the period of our initial baseline measurement in 1999. Worldwide, we estimate the total volume of VPN appliances (including firewall functions) will surpass \$285M (USD) in 2002 despite weakening resiliency of technology sector spending. The reason is two-fold: cognitive awareness for threats to enterprise security and a greater

outcrop of mobile employees with broadband network access requirements. And coupled to sharp declines in capital expenditures, more companies are realizing the need to move their infrastructure to remote locations for reasons of fiscal cost-cutting measures.

Not all VPN solutions create the same economic platform for scalable growth and management. WatchGuard Technologies has engineered their FireBox III and VClass family to capture a higher VPN density (number of synchronous tunnels) while accelerating throughput performance in the FireBox VClass by way of a custom security ASIC (application specific integrated circuit) design and chipset policy-based security functions. By embedding a portion of the security overhead on the firmware itself, the latency and performance losses can be minimized. This results in an actual gain for users in the VPN environment as packet congestion during peak usage can be effectively monitored and routed for a much-improved QoS function within the network.

And while most users would argue that quality is of lesser importance than reliability, network service providers have seen the critical advantage of properly allocated bandwidth in their offerings of VPN services to the SME (small-medium enterprise) marketplace. Quality of network services, and markedly in the VPN arena, relies on firmware solutions that embody both performance and security design. Nearly 63.2% of the studied organizations that use VPN gateways ranked QoS as their top evaluation criteria for selecting a VPN service provider (exclusive to external network service).

For producers of wholesale network services, the economic advantage is clearly seen through the ability to attract and sustain profitable network subscribers. And the capability to guarantee a measurable QoS service level agreement will be a competitive differentiation in next generation networks.

ServerLock and the Control of Intrusion Behavior

Intrusion Detection Systems (IDSs) yield the latest offering of safeguards against the risk of hacker penetration and the destruction of valuable information assets—exploited by design weaknesses in application and operating system architectures. And while some companies such as TripWire, Inc., offer products specifically appointed to the task of integrity monitoring, considerable effort should be placed on the *prevention* phase of any abnormal disruption. By abnormal disruption, this implies transforming information without malice but rather to mean incidental to the course of authorized IT users. This invokes a proactive assertion of control over files and system libraries versus a reactive detection to an intrusion incident—whereby damage can be done but after penetration.

WatchGuard's ServerLock™ application suite takes the problem of information invasion one step further to a rigid solution by establishing a secure core within each of the software's protected file assets. Control over any changes—whether by authorized or unauthorized user—is placed under an explicit lockdown function that prevents tampering by would-be exploiters. One of the remarkable behaviors that we observed in the study

population dealt with hacker activity that targeted file corruption for the sake of public vandalism. Of the total recorded external disruption violations, information vandalism received almost 21.7% of the attacks on organizations with greater than 500 employees. This means that the majority of SME businesses remain at risk for some type of vandal corruption—most commonly by Website but more often by information databases. Damages from information vandalism were estimated to cost businesses \$1,206M (USD) in 2001 for recovery of data and repair to information systems.

Expected to increase significantly in 2002 and beyond, these types of data corruption and intentional attacks can only be mitigated by placing barriers to entry inside of each and every information asset that requires integrity performance. After the fact of an incident is a moment too late when the damage has incurred and the recovery process begins.

Descriptive Statistics and the Economics of Network Violations

True costs of network disruptions—from multiple sources—has been historically difficult to measure and quantify since many of the repair costs are buried within the accounting systems of the victim organizations. And without an aggregated source of data relevant to such attacks, or statistical estimators that probe the ranges of actuarial cases, the design of macroeconomic interpretation was made on a lower confidence interval scale. Data is quite abundant and prominent code-level destruction spans the globe almost weekly. Anti-virus and pattern recognition companies such as Entercept and Symantec have carved a historian's position in recording the deluge of passive code-level attacks that flourish daily.

But in an economic sense, the real damage of attacks and malicious behavior takes shape as an *externality* of network-based computing. With open access to the Internet and information assets at risk, these attacks will continue to propagate and spread themselves in new hybrid platforms that will challenge the best firmware appliances and software developers alike.

Some of the empirically relevant figures and statistics that define this externality include:

- **Annual Cost of Network Breaches Worldwide: \$17,807M (USD) (2001, estimated)**
- **Average Cost of Network Breaches to Individual Organizations: 5.97% AGRP (2000), 6.27% (2001, estimated)**
- **Average Number of Breaches per Year Worldwide: 852,300 (Reported/Unreported)**
- **Average Cost of Virus or Worm Attack: \$26,271 (USD)**
(per incident, per company with greater than 150 employees)
- **Average Recovery Cost of a Network Breach: \$54,380 (Median Value)**
(per incident, per company with greater than 150 employees)
- **Average Wireless Revenue Assurance Loss: 4.72% of total call revenue**
(due to network fraud for an average U.S. wireless carrier)

Historical Lessons of Failure and Conclusion

Dating back to the early 1980's when hacker popularity began to rise, the commonality of PC security gave attention to the explosion of viruses that sprung up overnight in the midst of a booming personal technology revolution. Historical economists that look at past trends and determine their causal patterns have noted that malicious behavior coincides with peak economic periods during which significant advances in technology accompany surges in personal wealth. And next to these upturns in economic activity, vulnerability is at its highest level when organizations stay focused on wealth building activities and develop complacency for lax security procedures.

Today's technology has crossed over into new landscapes with network connectivity becoming central to emerging technologies in both enterprise and personal markets. This leads us to conclude that the network will be the most likely conduit for dispersal of passive code-level attacks and the Internet its global theater for terrorism in higher order. To protect against forthcoming intrusion and misappropriation of digital assets, organizations need to make a clear resolve in their expenditures toward security concentration within the network domain. Security is a rational element of business operations, but until recently, many had forgotten just how important this application could be in preserving the modern day enterprise.

Risk is always present at the epicenter of network computing and how a company faces risk can drastically alter their future. Begin by defining risk in terms that encompass your IT constituency. Then, use some of the parameters presented herein this appraisal to guide your measurement of the risk horizon. And once you determine the focus of risk mitigation, seek technologies that will serve an economic value in reducing that risk quotient.

Methodology

Conclusions and logical 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=3,286 companies) was queried from a previous data repository entitled, "Network Economics Study (2000-2002)", whereby we collected through primary 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 numerous analyses for logistic regression and CHAID relationships. To assess the implications of WatchGuard Technologies' solutions, we interviewed company personnel familiar with the technical performance and reviewed supporting documentation furnished by the respective product groups.

Choice sections of the resultant output has been shared in this report and serves as a definition of coefficient values used in conjunction with a separate user-driven tool, the WatchGuard Economic Calculator. These coefficients take shape in presenting a customized indication of the economic returns schedule for a given set of inputs. Please contact WatchGuard Technologies for access to this template tool.

About WatchGuard Technologies, Inc.

WatchGuard is a leading provider of dynamic, comprehensive Internet security solutions designed to protect enterprises that use the Internet for e-business and secure communications. The Company is a pioneer in the creation of the plug-and play Internet security appliance, the Firebox, and server security software. The Company's innovative LiveSecurity Service enables organizations and users to keep their security systems up-to-date, and its ServerLock and AppLock/Web software provide server content and application security to protect critical data and services against unauthorized or unintentional access or manipulation. The Company's RapidStream "Secured by Check Point" product line is specifically designed to address the enterprise customer's need for VPN performance, scalability, and flexibility in a Check Point appliance solution. For more information, please call 206-521-8340 or visit www.watchguard.com.

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 management.

No longer is market blindness an excuse, but rather an opportunity to witness the next horizon. Discover the insight of technology economics by visiting us on the Internet: <http://www.omniconsultinggroup.com>

vision
beyond
technology

www.technology-economics.com

About the Author

Frank J. Bernhard is 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 *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.



© 2002 OMNI Consulting Group LLP. All rights reserved.

OMNI Consulting Group LLP

Davis, CA 95616
Tel: 530.750.5199
Fax: 530.750.3710
information@ocg-us.com
www.omniconsultinggroup.com

WatchGuard, the WatchGuard logo, and all WatchGuard product names are trademarks of WatchGuard Technologies, Inc. Other brand and product names are trademarks of their respective holders. All specifications are subject to change without notice.