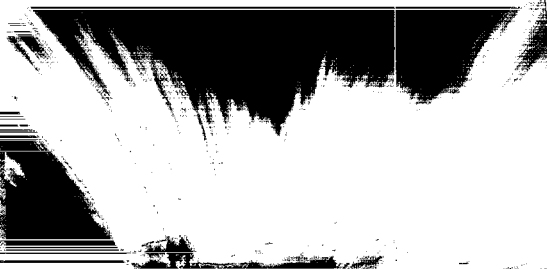




03058432

2002



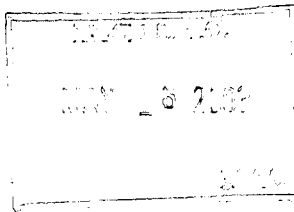
PROCESSED

MAY 09 2003

THOMSON
FINANCIAL

accelerating

WATCHGUARD TECHNOLOGIES, INC.



AR/S

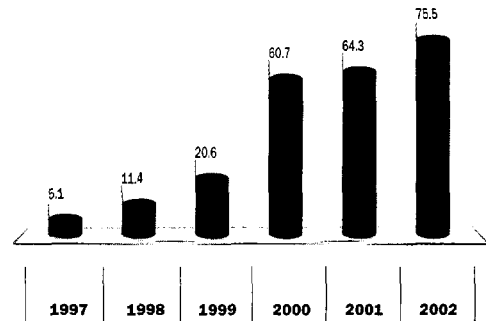
P.E. 12-31-02

WatchGuard

Financial Highlights

Annual Revenue

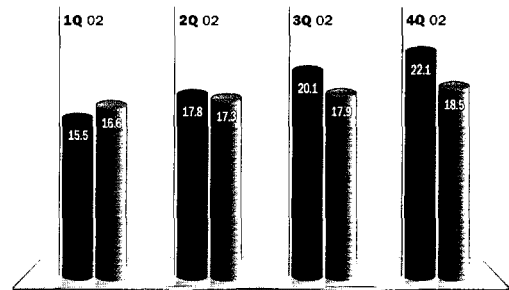
● Revenue



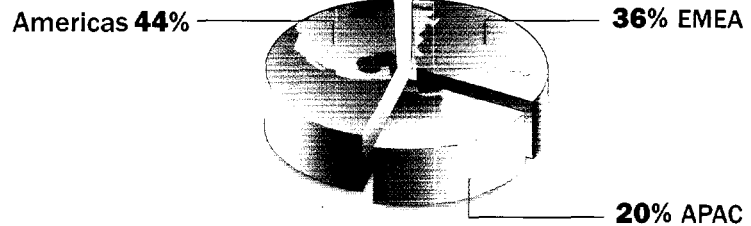
Quarterly Revenue and Deferred Revenue

● Revenue

● Deferred Revenue



Revenue by Region for 2002



Selected Financial Data

(amount in thousands, except per share data)

	1998	1999	2000	2001	2002
Net Revenue	11,379	20,619	60,703	64,283	75,500
Gross Profit	7,454	12,655	38,784	37,801	49,643
Loss From Operations	(9,000)	(16,173)	(21,964)	(42,591)	(34,487)
Net Loss	(9,119)	(16,018)	(15,664)	(36,977)	(31,596)
EPS	(11.34)	(1.80)	(0.66)	(1.38)	(1.02)
Shares Used in Calculating Net Loss Per Share	804	8,903	23,556	26,723	31,029
Cash and Equivalents	1,712	26,401	115,115	113,743	89,302
Total Assets	9,032	41,311	195,930	173,031	189,298
Deferred Revenue	1,841	4,233	11,874	15,709	18,451
Total Employees	88	165	287	298	331

Basic and diluted net loss per share is calculated by dividing net loss by the weighted average number of shares of common stock outstanding. Common stock equivalents, including preferred stock, stock options, and warrants, are excluded from the computation because their effect is antidilutive, except for pro forma earnings per share in 2000.

SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, D.C. 20549

FORM 10-K

FOR ANNUAL AND TRANSITION REPORTS
PURSUANT TO SECTION 13 OR 15(d) OF THE
SECURITIES EXCHANGE ACT OF 1934

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE
SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended December 31, 2002

OR

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE
SECURITIES EXCHANGE ACT OF 1934

For the transition period from _____ to _____

Commission file number 000-26819

WATCHGUARD TECHNOLOGIES, INC.

(Exact name of registrant as specified in its charter)

Delaware
(State or other jurisdiction of
incorporation or organization)

91-1712427
(I.R.S. Employer
Identification No.)

505 Fifth Avenue South, Suite 500, Seattle, WA 98104

(Address of principal executive offices) (zip code)

(206) 521-8340

(Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

None

Securities registered pursuant to Section 12(g) of the Act:

Common Stock, \$.001 par value

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports) and (2) has been subject to such filing requirements for the past 90 days. Yes No

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K.

Indicate by check mark whether the registrant is an accelerated filer (as defined in Exchange Act Rule 12b-2) Yes No

The aggregate market value of the voting and nonvoting common equity held by nonaffiliates of the registrant, based on the last sales price of the registrant's common stock on June 28, 2002, as reported on the Nasdaq National Market, was approximately \$141,543,691.

As of March 17, 2003, there were 32,828,311 shares of the registrant's common stock outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

The information required by Part III of this report, to the extent not set forth herein, is incorporated into this report by reference to the registrant's definitive proxy statement for the annual meeting of stockholders to be held on May 22, 2003. The definitive proxy statement will be filed with the Securities and Exchange Commission within 120 days after December 31, 2002, the end of the fiscal year to which this report relates.

WATCHGUARD TECHNOLOGIES, INC.
ANNUAL REPORT ON FORM 10-K
FOR THE FISCAL YEAR ENDED DECEMBER 31, 2002

TABLE OF CONTENTS

	<u>Page</u>
PART I	
ITEM 1. BUSINESS	3
ITEM 2. PROPERTIES	35
ITEM 3. LEGAL PROCEEDINGS	35
ITEM 4. SUBMISSION OF MATTERS TO A VOTE OF SECURITY HOLDERS	35
PART II	
ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY AND RELATED STOCKHOLDER MATTERS	36
ITEM 6. SELECTED FINANCIAL DATA	36
ITEM 7. MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS	38
ITEM 7A. QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK	56
ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA	57
ITEM 9. CHANGES AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURE	85
PART III	
ITEM 10. DIRECTORS AND EXECUTIVE OFFICERS OF THE REGISTRANT	86
ITEM 11. EXECUTIVE COMPENSATION	86
ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT	86
ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS	86
ITEM 14. CONTROLS AND PROCEDURES	86
ITEM 16. PRINCIPAL ACCOUNTANT FEES AND SERVICES	87
PART IV	
ITEM 15. EXHIBITS, FINANCIAL STATEMENT SCHEDULES AND REPORTS ON FORM 8-K ..	88

PART I

Forward-Looking Statements

Our disclosure and analysis in this annual report contain forward-looking statements, which provide our current expectations or forecasts of future events. Forward-looking statements in this annual report include, without limitation:

- information concerning possible or assumed future operating results, trends in financial results and business plans, including those relating to earnings growth and revenue growth;
- statements about our costs and operating expenses relative to our revenues and about the expected composition of our revenues;
- statements about our future capital requirements and the sufficiency of our cash, cash equivalents, investments and available bank borrowings to meet these requirements;
- information about the anticipated timing of new product releases;
- other statements about our plans, objectives, expectations and intentions; and
- other statements that are not historical facts.

Words such as “believes,” “anticipates” and “intends” may identify forward-looking statements, but the absence of these words does not necessarily mean that a statement is not forward-looking. Forward-looking statements are subject to known and unknown risks and uncertainties and are based on potentially inaccurate assumptions that could cause actual results to differ materially from those expected or implied by the forward-looking statements. Our actual results could differ materially from those anticipated in the forward-looking statements for many reasons, including the factors described in the section entitled “Important Factors That May Affect Our Business, Our Results of Operations and Our Stock Price” in this annual report. Other factors besides those described in this annual report could also affect actual results. You should carefully consider the factors described in the section entitled “Important Factors That May Affect Our Business, Our Results of Operations and Our Stock Price” in evaluating our forward-looking statements.

You should not unduly rely on these forward-looking statements, which speak only as of the date of this annual report. We undertake no obligation to publicly revise any forward-looking statement to reflect circumstances or events after the date of this report, or to reflect the occurrence of unanticipated events. You should, however, review the factors and risks we describe in the reports we file from time to time with the Securities and Exchange Commission, or SEC.

ITEM 1. BUSINESS

Overview

WatchGuard is a leading provider of Internet security solutions designed to protect enterprises that use the Internet for e-commerce and secure communications. Our mission is to provide enterprises worldwide with stronger Internet security solutions by offering integrated, multi-layered defenses and tools that protect against known and future threats in a smart way by including simplified implementation and management and proactive security with our LiveSecurity Service. With the risk that threats and attacks will compromise multiple points in a corporate network, the requirements of a security solution have expanded beyond the core requirement of firewalls for access control and virtual private networks, or VPNs, for secure communications. The comprehensive nature of an effective security solution, however, requires a robust and intuitive system that simplifies the implementation and management of the system. Because the security landscape is constantly evolving, an effective security solution must also be dynamic to allow an enterprise to keep its defenses ahead of the latest threats and attacks.

Thousands of enterprises worldwide use WatchGuard's award-winning products and services to address these challenges. These products and services include our high-performance Firebox and RapidStream firewall and VPN appliances for access control, secure communications and (with certain of our Firebox products) network-based intrusion protection capabilities, and our ServerLock technology and anti-virus solution for content and application security for servers and desktops with host-based intrusion protection capabilities. The centralized point-and-click management of our solutions allows even the non-security professional to effectively install, configure and monitor our security products while the networking features of our Firebox Vclass product line provide the functionality required for more complex network installations. In addition, our innovative subscription-based LiveSecurity Service enables our customers, with minimal effort, to protect their data and communications in a continuously changing environment.

Our core market spans the small- to medium-sized enterprise, or SME, market, from companies at the lower end, where ease-of-use is a key requirement, to companies at the high end, including those with high-speed connections supporting VPNs between the corporate headquarters and geographically dispersed branch offices, where performance, scalability and networking features are key requirements. In addition, with the recent addition of our RapidStream line of "Secured by Check Point" appliances, we also have the opportunity to leverage Check Point Software Technologies Ltd.'s established presence in the large enterprise market. Our security solutions also give enterprises a security management choice. An enterprise can manage its own Internet security with our product offerings or outsource its security management to an Internet service provider, or ISP, or other managed service provider implementing our managed security solutions. For the service provider, our technology improves the economics of managed security services through a scalable delivery platform that enables the service provider to remotely configure and manage thousands of customer sites quickly and easily.

We sell our Internet security solutions indirectly to end-users through thousands of distributors and resellers, with customers located in over 125 countries. We also sell directly and indirectly to a number of service providers that implement our managed security solution. As of December 31, 2002, we had shipped over 150,000 of our security appliances.

We initially incorporated in Washington in 1996 and reincorporated in Delaware in 1997. References to "we," "our," "us" and "WatchGuard" in this annual report refer to WatchGuard Technologies, Inc., our subsidiaries and our predecessor. Our executive offices are located at 505 Fifth Avenue South, Suite 500, Seattle, Washington 98104, and our telephone number is (206) 521-8340. We make available on our Web site, free of charge, copies of our annual report on Form 10-K, quarterly reports on Form 10-Q, current reports on Form 8-K, and amendments to those reports filed with or furnished to the SEC, as soon as reasonably practicable after filing or furnishing the information to the SEC. This information can be found in the investor relations portion of our Web site, which is located at www.watchguard.com. You may also inspect and copy the documents that we have filed with the SEC, at prescribed rates, at the SEC's Public Reference Room at 450 Fifth Street, N.W., Washington, D.C. 20549. You may obtain information regarding the operation of the Public Reference Room by calling the SEC at 1-800-SEC-0330. In addition, the SEC maintains a Web site that contains reports, proxy and information statements and other information regarding issuers that file with the SEC, at <http://www.sec.gov>.

Industry Background

Reliance on the Internet

The growth in the Internet has provided enterprises, regardless of size, with new revenue opportunities through global distribution of products and services and has enabled significant reductions in sales and marketing costs through automation and instantaneous access. Because of its affordability, global reach and versatility, the Internet is a particularly powerful and necessary tool for enterprises. Enterprises are increasingly required to establish secure Internet access to facilitate and support strategic business objectives. In a marketplace that is becoming more competitive, enterprises are increasingly utilizing new business tools and initiatives, such as remote access, e-commerce, online customer service and supply chain management to gain competitive advantage.

The need for Internet security

The increased importance of e-commerce and the proliferation and growth of corporate intranets have dramatically increased the openness of computer networks, with the Internet becoming a widely accepted platform for many business-to-business and business-to-consumer transactions. The accessibility and relative anonymity of users in open computing environments, however, make systems and the integrity of information stored on them increasingly vulnerable to security threats. Open systems present inviting opportunities for computer hackers, terrorists, curious or disgruntled employees and contractors, and competitors to compromise, alter or destroy sensitive information within the system or to disrupt operations and Internet access. In addition, open computing environments are complex and typically involve a variety of hardware, operating systems and applications supplied by a variety of vendors, making networks difficult to manage, monitor and protect from unauthorized access. In addition, because even smaller organizations are rapidly adopting public-facing Web and application servers, they now face the types of threats and vulnerabilities that had been previously reserved for much larger organizations that could deploy sufficient personnel to meet that challenge.

New attacks and security vulnerabilities are created or discovered on almost a daily basis. According to the Computer Emergency Response Team, a federally funded research and development center, not only is the number of cyber incidents and attacks increasing at an alarming rate, but the number of vulnerabilities is increasing as well. The number of vulnerabilities, or faults in software and hardware that may permit unauthorized network access or allow an attacker to cause network damage, has increased almost four-fold in two years, from 1,090 reported vulnerabilities in 2000 to 4,129 reported vulnerabilities in 2002. The annual Computer Security Institute, or CSI, survey conducted in 2002 highlights the potential risks faced by organizations connected to the Internet. The CSI survey revealed that 90% of companies responding had experienced security breaches and that 70% of these breaches were considered serious, with companies experiencing theft of proprietary information, financial fraud, or sabotage of data or networks. The average loss due to financial fraud or theft was estimated at over \$1 million. But the risks extend beyond outside attackers—71% of surveyed companies reported insider attacks. In addition to an increase in the number of attacks, the speed of propagation of these attacks is increasing as well. For example, NIMDA, an automated Internet attack that was a blend of a computer worm and a computer virus, spread across the United States in approximately one hour, lasted for days, and attacked approximately 86,000 computers. Code Red, another Internet attack, infected approximately 150,000 computer systems in approximately 14 hours. Organizations therefore often do not have the luxury of waiting for an alert about a current threat, but must be proactive in their defense against Internet security attacks.

The need for increased Internet security has been recognized at the highest national levels. In November 2002, President George W. Bush signed legislation creating the Department of Homeland Security. For fiscal year 2004, the Bush administration has requested \$4.7 billion for Internet security, up from \$4.2 billion in fiscal year 2003 and \$2.7 billion in fiscal year 2002.

The Internet security challenge

Adequate Internet security is not a response to a single challenge, but rather a response to a variety of business requirements. For example, because enterprises need to control the flow of information between their internal networks and the Internet, they need firewalls, which are important components of a comprehensive security solution. A firewall, a security component that varies in complexity, is designed to block access from the Internet to an enterprise's internal networks, as well as control the flow of and access to information shared between the networks and the Internet. A comprehensive security solution should also integrate several other sophisticated security layers, such as VPNs, to enable encrypted communications between points on the Internet, and content and application security for servers and desktops to protect critical data and services against unauthorized or unintentional changes.

Even a comprehensive solution, however, must be easy to install, configure and manage to be truly effective. With businesses increasingly establishing secure Internet access for branch offices, trading partners and traveling employees, an enterprise must deploy point solutions such as firewalls and VPNs to fully protect the

corporate network, as well as protect multiple servers and desktops in various locations. Without a robust, intuitive and easy-to-use system to manage these point solutions, the complexity and difficulty of successfully implementing a corporate information security solution rises dramatically.

To further complicate matters, the dangers against which an effective Internet security solution must protect are dynamic rather than static, with new types of intrusion schemes, worms, viruses and other security threats and vulnerabilities emerging constantly. CERT handled 82,094 security incidents in 2002, approximately 56% more than the 52,658 security incidents handled in 2001, and almost four times the 21,756 security incidents handled in 2000. In addition, unless an enterprise can timely and easily implement updates across the enterprise's point solutions protecting its network, the enterprise may need dedicated, and expensive, security experts to proactively identify, obtain and manually implement these updates quickly and correctly.

The Internet security opportunity

According to the *VPN and Firewall Products Quarterly Worldwide Market Share and Forecasts for 4Q02* report from Infonetics Research, Inc., "end-user demand is clearly a fundamental driver for deployment of VPN and firewall products, and demand is skyrocketing." Infonetics reports that the worldwide market for VPN and firewall appliances reached \$1.4 billion in 2002 and is forecasted to grow to \$2.2 billion in 2006, at a compound annual growth rate, or CAGR, of 22%. In addition, Infonetics believes that most end-users are moving from a model of centralized Internet connectivity to distributed connectivity, taking advantage of the cost savings offered by VPNs.

Enterprises require a robust, comprehensive Internet security solution that secures all vulnerable points in the corporate network, that can be installed, configured and managed easily, and that can be kept up to date quickly and effectively, all for an economical price. In addition, many enterprises would rather outsource the management of their Internet security to ISPs and other managed service providers. Service providers face challenges, however, in delivering affordable security services that can be rapidly and economically deployed to thousands of customer sites and easily managed from a central location.

The WatchGuard Solution

WatchGuard's security products and services offer an innovative approach to Internet security. Our solution has the following key benefits:

Stronger Security For enterprises of all sizes, we offer a strong, multi-layered defense and tools to protect against known and future threats. At its core, our solution includes a firewall for access control and filtering of dangerous content such as worms and viruses, and VPN capability for secure, encrypted communication between remote offices, mobile employees and trading partners. Beyond this, our solution provides network-based intrusion protection capabilities through WatchGuard's proxies and provides host-based intrusion prevention capabilities and server security to protect against unauthorized or unintentional access to and manipulation of critical content and applications residing on a server, such as Web site defacement and the deposit of malicious code. In addition, we offer proxies that are comprehensive and customizable, real-time network monitoring, dynamic content blocking, packet reassembly and scalable appliances. Finally, our solution provides an additional line of defense with signature-based anti-virus protection to secure the desktop.

Smartly Done We implement our security solution in a smart way with management tools geared toward the needs of the customer base they serve, quick and easy VPN creation and use, "drop-in" firewall configuration, comprehensive reporting, product bundles that simplify implementation and management and our unique LiveSecurity solution, all contained within a security appliance for ease of firewall and VPN deployment. Our subscription-based LiveSecurity Service is designed to keep our customers' security solutions up to date with

(1) information alerts that offer timely analyses of breaking Internet security news combined with instructions on how customers can keep their networks secure, (2) virus alerts with information from McAfee.com Corporation, or McAfee, that provide real-time virus alerts and specific information on how customers can protect their systems, (3) security threat responses that provide detailed information on high-profile security vulnerabilities as they develop, including information on how they may affect systems and what we are doing to help our customers keep their networks secure and, when appropriate, software updates to address the specific threat, (4) software updates, (5) support flashes with tips for managing WatchGuard products, (6) expert editorials to provide continuing education about Internet security, (7) Web-based and interactive technical support and (8) Web-based and interactive customer training.

Strategy

Our objective is to be the leading provider of Internet security solutions to SMEs worldwide and opportunistically expand our presence into other market segments. Our strategy to achieve these goals is based on the following key elements:

Continue to extend our leadership position in our core portion of the SME market and expand into the high end of the SME market with technological innovation

We intend to both solidify and further extend our SME market leadership position by expanding and enhancing our integrated Internet security solutions. We plan to accomplish this by increasing the breadth and depth of our multi-layered defense with additional intrusion detection and prevention, or IDP, technology, vulnerability assessment tools and services, and enhanced spam filtering and application layer security, while integrating these layers in a single, easily-managed appliance. Over time, we also intend to converge the security, management and hardware technology of our core product lines while preserving our existing customer base. This will allow us to provide higher performance appliances to the lower end of the SME market and increase the security features and functionality available to the higher end of the SME market, in addition to reducing our development and manufacturing costs and our time-to-market for future technology.

Expand, enhance and leverage our innovative LiveSecurity Service

Our subscription-based LiveSecurity Service is an innovative, value-added security service that provides information and virus alerts, threat responses, software updates, support flashes and expert editorials, along with training and technical support, over the Internet directly to our subscribers and service provider partners. We plan to expand and enhance our LiveSecurity Service, and therefore the value of our subscription service, by adding new software and services through internal development and partnering with third-party providers. We also intend to better leverage this relationship with our installed customer base by increasing the number of software and service add-ons sold through this service to these existing customers. As we expand and enhance our LiveSecurity Service, we plan to ensure that it remains easy to implement and use by enterprises of all sizes and by service providers.

Utilize our innovative ASIC-based hardware technology to differentiate and distance our solutions from our competition

We intend to utilize our innovative application-specific integrated circuit, or ASIC, architecture to facilitate the integration and efficiency of additional security layers in our easily-managed security appliance, while reducing our manufacturing costs and increasing our product development flexibility. We expect that our next-generation ASIC-based solutions will accomplish this with hardware designed to accelerate the performance of these additional layers without degrading the performance of the core firewall and VPN functionality and allow

“stacking” of multiple ASICs to leverage the same technology across a broad range of products. We believe this will allow us to provide a multi-layered defense integrated into an appliance that offers customers significant price and performance benefits.

Leverage third-party technology and resources to enhance our product offerings and penetrate the large enterprise market

In addition to utilizing internal development efforts, we plan to increase the breadth and depth of our multi-layered defense by leveraging the technology of third parties, which may involve either partnering or acquisition strategies. We also plan to continue to leverage Check Point’s established presence in the large enterprise market by making a Check Point software solution available on the same hardware platforms we utilize for our core product lines, which allows us to address a market we could not otherwise efficiently address. This strategy allows us to further increase our time-to-market and reduce our development risk while gaining the benefit of other parties’ expertise in particular technologies or markets.

Continue to expand WatchGuard brand awareness

We believe that we have an opportunity to make the WatchGuard brand synonymous with Internet security worldwide. We will continue to participate in public relations activities, seminars and trade shows, both domestically and abroad, to secure WatchGuard’s position as an expert and innovator in Internet and network security, as well as leverage our Web site and increase our end-user demand generation activities. Through online and print advertising, direct mail, e-mail and telemarketing campaigns, and particularly through our Web site and sales tools, we intend to leverage our marketing activities worldwide to uniquely position WatchGuard in the marketplace and clearly communicate the benefits of our comprehensive solutions to our customers and partners. We also intend to introduce innovative programs designed to simplify the purchase of our products, and to offer end-users product and service options that allow them to customize the solution to better address their needs. We will also strengthen our focus on specific vertical markets, such as state and local government agencies and education and health care organizations, to expand our customer base and provide the right solutions to address the special needs of these vertical markets.

We have not determined a schedule for implementing these components of our strategy. The timing for executing our strategies will depend on market conditions, the availability of strategic opportunities and the availability of management resources.

Products and Services

Our comprehensive security solutions include an integrated suite of security and management software, an Internet security appliance and a dynamic Internet-based service to keep security defenses current. These solutions provide access control, VPN, intrusion prevention capabilities and content and application security for servers and desktops. Enterprises may use our products to internally manage their Internet security or elect to outsource security management to a service provider implementing our managed security solution.

Security Layers

Firewall and VPN

By using our Firebox products, an enterprise can quickly and affordably deploy comprehensive perimeter security protection and VPN capability across its network, but still retain centralized control and administration. In addition, our LiveSecurity Service enables enterprises to augment their information technology staff with our security experts, which we believe substantially reduces personnel costs. Our Firebox III products include an initial one-year subscription to our LiveSecurity Service and our Firebox SOHO and Firebox Vclass products include an initial 90-day subscription to our LiveSecurity Service.

We currently offer the following Firebox III/Firebox SOHO and Firebox Vclass models:

Firebox Model	Firebox 4500	Firebox 2500	Firebox 1000	Firebox 700	Firebox 500	Firebox SOHO 6 & SOHO 6tc
Recommended For	Corporate Headquarters and Large Enterprises, Wire Speed VPN Support	Medium to Large Enterprises, High Volume Web Traffic	Mid-Size Business or Branch Office	Smaller Business or Remote Office	Stand-Alone Firewall for Small Office	Small Stand-Alone or Remote Office
Authenticated Users	5000	5000	1000	250	250	10 (upgrades to 50)
User License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	10 (upgrades to 50)
Firewall Throughput	200 Mbps	200 Mbps	200 Mbps	150 Mbps	75 Mbps	75 Mbps
VPN Throughput (3DES Encryption + SHA1)	100 Mbps	75 Mbps	60 Mbps	5 Mbps	5 Mbps	20 Mbps
Hardware Encryption Acceleration	Yes	Yes	Yes	No	No	Yes
Branch Office/ Mobile User VPNs	3000**	2000**	1300**	150**	50**	6*
Interfaces	Three RJ-45 10/100TX Ethernet, DB-9 Serial Port, PCI Expansion Option	Three RJ-45 10/100TX Ethernet, DB-9 Serial Port, PCI Expansion Option	Three RJ-45 10/100TX Ethernet, DB-9 Serial Port, PCI Expansion Option	Three RJ-45 10/100TX Ethernet, DB-9 Serial Port	Three RJ-45 10/100TX Ethernet, DB-9 Serial Port	6 RJ-45 10BaseT Ethernet

* Included in SOHO 6tc; optional on SOHO 6

** Total number of Branch Office plus Mobile User VPN Tunnels

Firebox Vclass Models	Firebox V200*	Firebox V100	Firebox V80	Firebox V60	Firebox V60L	Firebox V10
Recommended For	VPN concentrator, data center firewall, multi-tenant security	VPN concentrator, data center firewall, multi-tenant security	High-speed VPN tunnel connecting data centers, data center firewall, Fast Ethernet firewall, multiple T3 firewall	VPN concentrator, Fast Ethernet firewall, HQ for SMEs	VPN concentrator, mid-sized enterprise	Small standalone or branch office firewall and VPN
Concurrent Sessions	500,000	250,000	128,000	16,000	8,000	2,000
User License	Unlimited	Unlimited	Unlimited	Unlimited	250	Unlimited
Firewall Throughput	2Gbps	600 Mbps	200 Mbps	200 Mbps	100 Mbps	75 Mbps
VPN Throughput (3DES Encryption + SHA1)	1.2 Gbps	300 Mbps	150 Mbps	100 Mbps	50 Mbps	20 Mbps
Hardware Encryption Acceleration	Yes Proprietary Intelligent ASIC	Yes Proprietary Intelligent ASIC	Yes Proprietary Intelligent ASIC	Yes Proprietary Intelligent ASIC	Yes Proprietary Intelligent ASIC	Yes Proprietary Intelligent ASIC
Branch Office VPNs	40,000	20,000	8,000	400	50	10
Interfaces	2 x 1000 BaseSX Gigabit, 2 x High Availability (Ethernet) ports, 1 x console port	2 x 1000 BaseSX Gigabit, 2 x High Availability (Ethernet) ports 1 UPS port 1 x console port	4 x 10/100 Ethernet, 2 x High Availability (Ethernet) ports 1 UPS port 1 x console port	4 x 10/100 Ethernet, 2 x High Availability (Ethernet) ports 1 UPS port 1 x console port	4 x 10/100 Ethernet, 2 x High Availability (Ethernet) ports**	2 x 1000 BaseSX Gigabit, 1 x RS232 console port

* Expected availability early-to mid-2003

** High availability optional on Firebox V60L

RapidStream currently offers the following models:

RapidStream Model	RapidStream 11000	RapidStream 8100	RapidStream 6100	RapidStream 2200*	RapidStream 2100
Recommended For	Large central enterprise sites, data centers, Web hosting, service providers, e-commerce	Central corporate sites with expanding traffic requirements, service providers, e-commerce	Growing enterprises with VPN connectivity to remote sites and partners, corporate office, e-business	Lower mid-size enterprises as a VPN concentrator, satellite branch offices, meshed VPN site	Lower mid-size enterprises as a VPN concentrator, satellite branch offices, meshed VPN site
Concurrent Sessions	200,000	128,000	64,000	8,000	8,000
User License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Firewall Throughput	2.0 Gbps	600 Mbps	200 Mbps	200 Mbps	200 Mbps
VPN Throughput (3DES Encryption + SHA1)	1.2 Gbps	300 Mbps	160 Mbps	120 Mbps	70 Mbps
Hardware Encryption Acceleration	Yes Proprietary Intelligent ASIC	Yes Proprietary Intelligent ASIC	Yes Proprietary Intelligent ASIC	Yes Proprietary Intelligent ASIC	Yes Proprietary Intelligent ASIC
IPSec Tunnels	40,000	20,000	8,000	400	400
Interfaces	2 x 1000 BaseSX Gigabit ports, 2 x High Availability (10/100 Ethernet) ports, 1 x DB-9 console port	2 x 1000 BaseSX Gigabit ports, 2 x High Availability (10/100 Ethernet) ports, 1 UPS port, 1 x DB-9 console port	3 x 10/100 Ethernet ports, 2 x High Availability (10/100 Ethernet) ports, 1 x UPS port, 1 x DB-9 console port	4 x 10/100 Ethernet ports, 2 x High Availability (10/100 Ethernet) ports, 1 x UPS port, 1 x RJ-45 console port	3 x 10/100 Ethernet ports, 1 x UPS port, 1 x RJ-45 console port

*RapidStream 2200 currently available in North America and Europe only

Server Security

For enterprises of all sizes, the ServerLock System provides host-based intrusion protection capabilities and server content and application security that protects critical data and services against unauthorized or unintentional access or manipulation, such as Web site defacement and the deposit of malicious code. This protection is offered through a combination of kernel-level software, secured remote communications, centralized management and a simplified dual-mode administrative model. We also offer an application-specific version of our server security software for Web sites residing on a Windows NT or Windows 2000 server using Microsoft IIS. Every standard ServerLock System product includes an initial one-year subscription to our LiveSecurity Service. We currently offer the following server security products:

- ServerLock for NT/2000;
- ServerLock for Solaris; and
- AppLock/Web.

Desktop Security

Through our relationship with Network Associates, Inc., we currently offer desktop virus protection with the McAfee Virus Scan ASaP product for Microsoft Windows 98, NT and 2000 operating systems. Every standard Firebox product includes either one annual Virus Scan ASaP license for our SOHO-class Firebox products or five annual Virus Scan ASaP licenses for all of our other Firebox products. Additional licenses may also be purchased separately.

Security Layer Management and Monitoring

We offer robust and intuitive management and monitoring of our comprehensive Internet security layers that reduce the complexity and difficulty of successful implementation and provide for better visibility of the security environment. Our management and monitoring tools include:

- *Control Center.* Our easy-to-use Control Center management tool serves as the operational headquarters for the Firebox III products. The Control Center is designed to enable the end-user to quickly and easily configure the Firebox III product, implement security policies and monitor the status of installed network services.
- *Global Policy Manager.* Centrally located at a managed security service provider's network operations center, our Global Policy Manager for our Firebox III and Firebox SOHO line of products provides security intelligence and configuration for all customer sites under management. Global Policy Manager allows the service provider to create and store various security policy configurations for different customer groups or service plans.
- *Logging, Notification and Monitoring.* For the Firebox III and Firebox SOHO products, the following tools are also available:
 - *Firebox Monitors:* Integrated monitoring and reporting tools for the Firebox III products provide real-time and historical data about network traffic and allow customers to detect and interrupt suspicious activity.
 - *Logging and Notification:* The Firebox III products support multiple levels of logging and notification while the Firebox SOHO product supports a more limited form of logging. Logs from multiple sites can be securely distributed to a central location using 3DES encryption.
 - *HostWatch:* HostWatch displays real-time monitoring of network usage mapped to authenticated users and host computers. Color-coded connection types (Allowed, Denied, Proxied or Masqueraded) between internal and external hosts are identified by IP address, DNS name or user name.
 - *Historical Reporting:* Our flexible HTML-based historical reporting tool for the Firebox III products enables end-users to summarize network activity through custom and standardized reporting options.
- *VPN Manager.* VPN Manager automates the creation of VPN tunnels between an enterprise's headquarters, branch offices and remote users utilizing Firebox III and Firebox SOHO products, and is designed to dramatically reduce the complexity of creating and managing multi-site VPNs. With VPN Manager, VPN tunnels can be created with a revolutionary quick and simple point-and-click user interface.
- *Vcontroller.* A comprehensive, cross-platform Firebox Vclass appliance management console, the Vcontroller provides for the configuration of firewall and VPN policies and provides access to all the enterprise-class features of the Firebox Vclass appliance, such as:
 - Firewall, network address translation and VPN policies;
 - Quality of service, VLAN, server load balancing and remote user policies;

- Real-time monitoring of traffic statistics;
- Configurable alarm and event notification; and
- Configurable logging.
- *Central Policy Manager.* Central Policy Manager, or CPM, is a powerful, scalable network management platform designed to simplify large-scale deployment, configuration and monitoring of firewall and VPN features for Firebox Vclass appliances. CPM compiles network-wide security policies into individual appliance policies, automatically taking into account the relationship between different appliances. This allows CPM to effectively and efficiently manage even hundreds of security appliances.
- *ServerLock Manager.* The ServerLock Manager is designed to maximize efficiency of control for tens and even hundreds of servers, all using secure, remote communication channels. The ServerLock Manager allows administrators or service providers to control multiple servers by applying custom rules and turning protection on and off in much the same manner as if those tasks were performed locally. ServerLock's remote communications channel is designed to simplify setting and resetting the protection state of remote machines and to make aggregating systems easier, which provides simplicity of depiction in a managed environment.

LiveSecurity Service

Our subscription-based LiveSecurity Service for both enterprises and managed security providers and their customers includes (1) information alerts that offer timely analyses of breaking Internet security news combined with instructions on how customers can keep their networks secure, (2) virus alerts with information from McAfee that provide real-time virus alerts and specific information on how customers can protect their systems, (3) security threat responses that provide detailed information on high-profile security vulnerabilities as they develop, including information on how they may affect systems and what WatchGuard is doing to help its customers keep their networks secure and, when appropriate, software updates to address specific threats, (4) software updates, (5) support flashes with tips for managing WatchGuard products, (6) expert editorials to provide continuing education about Internet security, (7) interactive and Web-based technical support and (8) interactive and Web-based customer training. We currently offer standard and enhanced versions of our LiveSecurity Service, each of which provides end-users with differing levels of interactive technical support:

Standard Technical Support Service

- Access to a moderated online user forum;
- Technical support 12 hours a day, five days a week (based on the customer's local time);
- Target four-hour maximum response time for customer service; and
- Access to technical support team, limited to three to five incidents per year (depending on the product).

Gold Technical Support Service Upgrade

- Access to a moderated online user forum;
- Technical support 24 hours a day, seven days a week;
- Target one-hour maximum response time for customer service; and
- Unlimited access to technical support team.

Other Products

We offer additional products and options, including

- Mobile-user VPN for telecommuting or traveling employees;

- High Availability for security appliance failover protection;
- Web-Blocker to restrict Web site access;
- VPNForce upgrades to apply corporate policies to telecommuter workstations, secure wireless connections and create secure branch office VPNs that are separate from an enterprise's trusted network;
- Dual ISP Port Upgrade failover protection;
- SpamScreen to filter or identify email spam; and
- User upgrades for all of our Firebox SOHO products.

Customer Service

We make customer service a priority and consider it a competitive advantage for WatchGuard. Our staff of technical support representatives serves our end-users and our reseller, distributor and service provider partners by phone and via the Internet. Support is available to our partners that have representatives who have passed required WatchGuard technical training. For our end-users, we offer the two technical support programs described above, our Standard Technical Support Service and our Gold Technical Support Service Upgrade. In addition to the WatchGuard technical support staff, we offer all authorized WatchGuard customers access to our Web-based technical support self-help toolset 24 hours a day, seven days a week. These tools include comprehensive frequently asked questions, a listing of all known issues with our current software version (and any available work-arounds or fixes), and an interactive Web forum that allows customers to post WatchGuard-related technical questions to other customers and the WatchGuard technical moderator.

The WatchGuard Team of Experts

Rapid Response Team. Our rapid response team identifies, analyzes and generates responses to new Internet security threats. To identify new threats, the team monitors a wide variety of Internet sources related to network security, including newsgroups, vendor Web sites and security-related bulletin boards. When the rapid response team identifies a new security threat, we send an advisory to our LiveSecurity Service subscribers informing them of what they need to do to keep their system secure and, if appropriate, provide software updates that address the threat. The team also provides other information of interest relating to Internet security.

LiveSecurity Advisory Council. Our LiveSecurity Advisory Council provides continuing education and editorials on the rapidly changing subject of Internet security. The Council also contributes to the efforts of our rapid response team. Currently, the LiveSecurity Advisory Council is composed of Jack Danahy, Rik Farrow and David Piscitello.

Jack Danahy. Formerly Vice President of Server Security at WatchGuard, Jack Danahy has more than 15 years of engineering and business development experience. Mr. Danahy founded Qiave Technologies Corporation, which was subsequently acquired by WatchGuard. Mr. Danahy is a frequent speaker on Internet security topics and has been a contributor to the U.S. Army War College, the Center on Law, Ethics and National Security, the 1997 President's Commission on Critical Infrastructure Protection and the House Subcommittee on Information Technology. He is a charter member of the International Computer Security Association consortia on cryptography and ISP security and a member of the High Technology Crime Investigators' Association. Mr. Danahy holds patents or has patents pending in kernel security, secure remote communications, systems management and distributed computing.

Rik Farrow. Mr. Farrow provides UNIX and Internet security consulting and training. He has been working with UNIX system security since 1984 and with TCP/IP networks since 1988. He has taught in a number of countries and for a variety of organizations, and consults with firms in designing and implementing

security applications. Mr. Farrow is the author of *UNIX System Security* and is the co-author, with Rebecca Thomas, of *UNIX Administrator's Guide to System V*. He writes a column for *login:*, the magazine of the USENIX Association, and a network security column for *Network* magazine.

David Piscitello. Mr. Piscitello is an internationally recognized expert in internetworking and fast-packet technology. He founded Core Competence, a full-service internetworking, broadband, security and network management consulting firm with offices in Pennsylvania and South Carolina. He is the recipient of a Bellcore President's Recognition Award for his contributions to SMDS, or Switched Multimegabit Data Service, ATM, or Asynchronous Transfer Mode, and customer network management for switched data services. Mr. Piscitello has authored books on internetworking and remote access and publishes articles regularly on a variety of subjects, including network security, wireless data networking, switched internetworking, Internet security and VPNs. Mr. Piscitello does testing, product reviews and evaluations of VPNs, firewalls, intrusion detection and other security products for leading trade publications and consults for Fortune 100 companies on extranets and Internet security. He is chairman of the Network + Interop Program Committee and the founder and program chairman of the Internet Security Conference.

Licensing and Pricing

We offer our resellers, distributors and service provider partners discounts from our suggested retail prices. In addition, we offer educational discounts and promotional pricing as appropriate. All customers purchasing our Firebox and ServerLock products receive a perpetual license for our security and management software, which is included in the system price. Depending on the product purchased, each end-user purchaser of our standard products also receives a renewable one-year or 90-day subscription to our standard LiveSecurity Service. For our managed security solution, the service provider buys a license to use our network operations center security suite management and security software. In addition, the service provider must have an active subscription to the LiveSecurity Service for each end-user security appliance that it manages.

Sales, Marketing and Distribution

Because the need for Internet security crosses geographic and economic boundaries, our business opportunity extends worldwide to all business segments. Since our inception, we have invested heavily in worldwide sales and marketing. International sales generated 56% of our revenues in 2001 and 58% of our revenues in 2002.

We sell our security solutions through distributors, value-added resellers, or VARs, and service providers. We also sell our managed security solution products and services directly to service providers. We resell our products and services directly and indirectly through distributors, resellers and service providers, including

- distributors, such as Ingram Micro, Otsuka Shokai Co., Tech Data, Wick Hill Group, Westcon, Alternative Technologies and Compushack;
- VARs, such as XO Communications, Secure Networks Ltd., Century Computing Ltd., Siemens Business Services, Taskarena IT-Solutions GmbH, Nextcom, Softbank, Fujitsu Business Systems, Ltd. and Network Computing Architects, Inc.;
- direct marketers, such as CDW Computer Centers, Insight Enterprises, Dell, Microwarehouse and PC Connection; and
- service providers, such as AT&T Global Network Services Hong Kong Limited (AGNS Ltd.), Deutsche Telekom, Internet Initiative Japan, Internet Security Systems, KPN, Nextcom, Sunrise Communications, Easynet and Star Internet.

As part of our distribution network, thousands of resellers worldwide sell our security solutions. In 2002, we significantly realigned our channel network to focus our efforts on channel customers capable of assisting us in growing our business and expanding our reach into the higher end of the SME market and required many of our

smaller channel customers to purchase our products and services through our established distribution partners. One of the key programs we implemented worldwide in our reseller channel to implement this realignment was our authorized reseller program, called the WatchGuard Secure Partner Program, or WSP Program. The WSP Program offers programs and financial benefits to security-focused resellers who meet technical and sales certifications and promote WatchGuard to end-users. At the end of 2002, we authorized over 500 WatchGuard Secure Partners worldwide. Our agreements with our distribution network are nonexclusive. As of December 31, 2002, we had shipped over 150,000 of our security appliances to our distribution network, which resells our products and services to end-users spanning a wide variety of industries and more than 125 countries.

We divide our sales organization geographically and by channel customer focus. We have sales teams specifically responsible for the Americas, Europe/Middle East/Africa and Asia Pacific. Our sales professionals are typically local nationals who live and work in their designated geographic regions. We also assign sales resources to specific channel categories, including distribution, resellers and managed security providers. In the Americas, our national account managers are responsible for our relationships with our distribution network, helping them sell and support key reseller accounts and acting as a liaison to our marketing and product development organizations. Our enterprise sales team works directly with resellers who purchase through distribution. The enterprise sales team recruits new resellers, provides training on WatchGuard products and assists in selling to end-user customers.

We have a dedicated channel marketing team responsible for delivering programs, sales tools and communication specific to the categories of channel customers. The team supporting national accounts works closely with distributors to market our products to their resellers through advertising, e-mail, training opportunities and seminars. The team supporting enterprise accounts promotes and manages the WSP Program, organizes training seminars and assists with co-marketing opportunities presented by our resellers. We actively participate in public forums to inform existing and potential end-user customers, distributors, resellers and service providers about the capabilities and benefits of our products. These include industry trade shows in every major geographic region, product technology conferences, regional awareness programs, trade publications and journals. We use the Web extensively to deliver information to both end-users and our channel customers and have a dedicated, secure Web site that provides extensive information to channel customers. We offer resellers access to white papers, competitive information, graphics to assist their advertising efforts, product and sales training modules and the opportunity to post information about their events online. In addition, partners receive communications from us through the LiveSecurity Service.

We offer comprehensive online training on our security solutions through our Web site. Our interactive training system guides both end-user customers and resellers through the installation, setup and management of our Firebox security solutions and provides new product information. Training modules cover firewall basics, VPN, server security and sales training (for resellers only), and include live-action video and audio question-and-answer segments. Online certification testing is offered for both end-user customers and resellers to confirm their product knowledge.

The growth rate of our domestic and international sales has been and may in the future be lower in the summer months, when businesses often defer purchasing decisions. Also, as a result of customer buying patterns and the efforts of our sales force to meet or exceed quarterly and year-end quotas, historically we have received a substantial portion of a quarter's sales orders and earned a substantial portion of a quarter's revenues during the quarter's last month and the latter half of the last month.

Technology and Architecture

Firebox III and Firebox SOHO Products

For smaller enterprises, or those that require an easy-to-use solution, the Firebox III and Firebox SOHO products provide access control and VPN through three key components: our security management system

software with security and management features, our security appliance and a subscription to our Internet-based LiveSecurity Service.

Security features. The Firebox III and Firebox SOHO products contain the following security features:

- *Firewall.* Our firewall controls incoming and outgoing traffic between the Internet and an enterprise's systems and data. The firewall incorporates access control and detection and blocking features.
- *Authentication.* In our Firebox III products, our authentication features identify network users and define user and user-group security policies.
- *Virtual private networking.* Using encryption technology, our software enables enterprises to create VPNs, which allow data to flow securely across the Internet between two predetermined points. Our branch office VPN, which is included in all of our Firebox III and Firebox SOHO products, secures communications with branch offices and trading partners. Our remote-user VPN, included in our Firebox III products, secures connections to telecommuters and traveling employees. Our VPN solutions implement industry standard protocols such as IPSec, IKE and PPTP.
- *Network Address Translation.* Network address translation, or NAT, enables users to hide their internal IP addresses and allows internal servers with unregistered IP addresses to function as Internet-accessible servers, which increases network security. The Firebox III and Firebox SOHO products support static, dynamic, real one-to-one NAT, and can be configured to serve DHCP addresses.
- *Web surfing control.* In our Firebox III products, our Web-blocking feature enables enterprises to restrict site access privileges by user, group, time of day, site type or particular site. In our Firebox SOHO products, Web site access privileges may be restricted simply by site type.
- *Security appliance.* Our Firebox III and Firebox SOHO security appliances are dedicated solely to running security functions and IP sharing and have no other function and no hard drive memory storage. Our Firebox III products are standalone Internet security appliances that run the security functions of the product line. The security capabilities of these security appliances come entirely from the operating system, security software and security policies directed to them from the remote management software. They simply plug in and reside between an enterprise's Internet router and its internal network of servers and workstations. These security appliances have three independent, separately monitored connections: one to the enterprise's network, one to the Internet and one to the enterprise's public network for hosting Web and e-mail servers. The Firebox III products encrypt communications between the security appliance and the management software on the in-house manager's desktop. Our Firebox SOHO products are standalone Internet security appliances that run security functions and provide IP sharing. Our Firebox SOHO appliances are increasingly being used by enterprises as endpoints for VPNs. The security capabilities of the Firebox SOHO security appliances come entirely from the operating system, security software and security policies that reside on the appliances or that the appliances receive from remote management software. They simply plug in and reside between the Firebox SOHO's or telecommuter's Internet router and broadband modem and its internal network of servers and workstations. These security appliances have up to three independent, separately monitored connections: one to the Firebox SOHO's or telecommuter's network, one to the Internet and, optionally, one for a second failover Internet connection, or separate secondary telecommuter network where encryption can be enforced.

Our Firebox III and Firebox SOHO products utilize an innovative distributed architecture through which a basic processor in a security appliance receives and executes software directed to it from a remote management system. This technology allows us to keep our customers' security up to date with our LiveSecurity Service, which provides new security software and operating system configurations while still enabling us to take advantage of hardware acceleration for key functions.

Our Firebox III and Firebox SOHO products encrypt communications between WatchGuard, the management system software and the security appliance. This allows the management system and the appliance to be separated within an enterprise's local- or wide-area network or between a service provider and its subscriber. Typically, to install software on a computer using a general-purpose operating system such as Windows, a person must be physically present at the computer. Our distributed architecture, however, allows our customers to remotely install our software on the security appliances and receive our LiveSecurity Service over the Internet, thereby eliminating the need for someone to be physically present at each location.

Operating system software. Our Firebox III products use a Linux operating system and our Firebox SOHO products use a VxWorks operating system. For the Linux operating system, we use a custom-configured kernel under an open source license, which enables us to review the source code and generate a flexible, robust and secure operating system. We use specially designed application programming interfaces in all of our Firebox III and Firebox SOHO products to facilitate secure loading of the operating system and security software that our management software sends to the appliance.

Security feature implementation. The Firebox III and Firebox SOHO products implement our security features through a number of software modules. Each module provides the specific function that the management system defines in security rules and transmits to the appliance. For example, the firewall features that control network traffic are based on an extensible set of network service protocols, such as HTTP (Web traffic) and SMTP (e-mail). Our firewall differs from other appliance firewalls in that we provide two different levels of protection, stateful packet filtering, which has become the de facto standard in the industry, plus transparent application proxying that allows us to examine the content of a data stream in detail and provide enhanced protection against specific threats that stateful packet filters cannot detect. This is particularly important for the four key business protocols, HTTP, SMTP, FTP (file transfer) and DNS (Internet name services). The Firebox III or Firebox SOHO appliance applies the security policies defined by the management system to all incoming or outgoing traffic. Additional modules implement other security features, such as authentication and Web-surfing control, which also are defined in the security policies that the management system transmits to the appliance. If Web-surfing control is activated, for example, the Web-surfing control software module will automatically check the details of all outgoing Web traffic to make sure it complies with the defined policies.

We use an open architectural structure to allow integration with common standards for network security. For example, our VPN component currently supports IPSec and IKE standards and the authentication module in our Firebox III products supports a variety of standard authentication methods. We intend to adopt additional standards as they mature in the market.

Management features. Our management software allows a customer to manage and monitor the enterprise's Internet security with an intuitive, point-and-click user interface.

Integrated suite of system management tools. Our Firebox III products use a Windows-based security management system that packages, configures and deploys security software, security policies and the operating system from the in-house manager's desktop computer to the enterprise's security appliances. The management system also includes logging and notification functions and real-time monitoring and historical reporting of network, service and bandwidth usage. Our Firebox SOHO products are managed by a Web-based interface accessed from the appliance itself or from remote management software. Our management tools allow the management of multiple security appliances from a single location.

Because enterprise, distributed VPN and service provider environments are very different, we designed separate management systems for each. Our Firebox III and Firebox SOHO management software enables quick installation and management by an in-house manager using a standard Windows-based system. The VPN management software in each of our security appliance types is designed specifically for ease of configuration and visual representation of multiple VPNs in a network. We designed our managed security solution management software, on the other hand, for a trained operator using a dedicated management console to

configure and manage the security of a large subscriber base. All management systems have the ability to remotely deploy new security software to the appliances or update their security engines from the management console. Our SOHO and telecommuter customers can also choose a simple Web-based management interface, which removes the need to install management software.

Automated installation guides. Our automated installation guides enable enterprises to install and configure our systems in as quickly as 15 to 30 minutes. Software updates or upgrades are also accessed through easy-to-use installation guides.

Firebox Vclass Products

For larger enterprises, or for those that require greater performance, scalability and networking features, our Firebox Vclass products provide access control and high-performance VPN through three key components: our security management system software with security and management features, our security appliance and a subscription to our innovative LiveSecurity Service.

Security and networking features. The Firebox Vclass products contain the following security and networking features:

- *Firewall.* Our firewall controls incoming and outgoing traffic between the Internet and an enterprise's systems and data. The firewall incorporates access control and detection and blocking features. The filters track which computer is sending what traffic, and what type of traffic should typically come next. Based on what the next expected packet should look like in a normal session, stateful packet filtering can instantly create new accept-or-deny rules.
- *Authentication.* Our authentication features identify network users and define user and user-group security policies.
- *Virtual private networking.* Using encryption technology, our software enables enterprises to create VPNs, which allow data to flow securely across the Internet between two predetermined points. Our branch office VPN, which is included in all of our Firebox Vclass products, secures communications with branch offices and trading partners. Our Mobile User VPN, which is included in our Firebox V100, V80, and V60 models, secures connections to telecommuters and traveling employees. Our VPN solutions implement industry standard protocols such as IPSec, IKE and PPTP.
- *Network Address Translation.* NAT enables users to hide their internal IP addresses and allows internal servers with unregistered IP addresses to function as Internet-accessible servers, which increases network security. The Firebox Vclass products support static, dynamic, real one-to-one NAT, subnet-to-subnet, port forwarding and Virtual IP.
- *Traffic Management Quality of Service.* Firebox Vclass products provide policy-based traffic management and Quality of Service, or QoS. With weighted fair queuing, policies are prioritized and provisioned. Users can overwrite DiffServ Codepoint, or DCSP, and Type of Service, or ToS, marking for inbound and outbound traffic flow to qualified packets. Traffic Management QoS enables the Firebox Vclass appliances to participate in Multi Protocol Label Switching, or MPLS, environments and provides additional QoS.
- *Server Load Balancing.* To ensure that mission-critical resources remain available, the Firebox Vclass products distribute traffic to up to 16 servers. Traffic is then balanced between available servers using six common algorithms: round-robin, weighted round-robin, random, weighted random, least connections, and weighted least connections.
- *Security appliance.* Our security appliances are dedicated solely to running security functions and IP sharing and have no other function and no hard drive memory storage. Our Firebox Vclass security appliances are stand-alone Internet security appliances that run the security functions of the products. The security capabilities of these security appliances come entirely from the operating system, security

software and security policies directed to them from the remote management software. They simply plug in and reside between an enterprise's Internet router and its internal network of servers and workstations. These security appliances have three independent, separately monitored connections: one to the enterprise's network, one to the Internet and one to the enterprise's public network for hosting Web and e-mail servers. The Firebox Vclass products encrypt communications between the security appliance and the management software on the in-house manager's desktop.

Our Firebox Vclass products use a high-speed custom security ASIC processor featuring our cut-through architecture. With this architecture, the first packet or first few packets of a connection are forwarded to the firewall/VPN software to find the matching policy action. Once a policy decision is made, the policy actions are downloaded to the security ASIC processor so subsequent policy actions of the same connection can be processed in the high-performance security ASIC processor. This cut-through architecture not only improves firewall and VPN performance, but also leaves the central processing unit more bandwidth to process logging and other management tasks. The security ASIC processor accelerates firewall, VPN, NAT and QoS functionalities. The security ASIC processor also has four embedded RISC processors for greater feature flexibility to meet the needs of the most demanding network security applications.

Our Firebox Vclass products encrypt communications between corporate offices and between the appliance and the management software. This allows the management system and the appliance to be separated within an enterprise's local- or wide-area network or between a service provider and its subscriber. Typically, to install software on a computer using a general-purpose operating system such as Windows, a person must be physically present at the computer. Our distributed architecture, however, allows our customers to remotely install our software on the security appliances and receive our LiveSecurity Service over the Internet, thereby eliminating the need for someone to be physically present at each location.

Operating system software. Our Firebox Vclass products incorporate a Linux operating system using a custom-configured kernel under an open source license, which enables us to review the source code and generate a flexible, robust and secure operating system. We use specially designed application programming interfaces in all of our Firebox Vclass products to facilitate secure loading of the operating system and security software that our management software sends to the appliance.

Security feature implementation. Our Firebox Vclass products implement our security features through a number of software modules. Each module provides the specific function that the management system defines in security rules and transmits to the appliance. For example, the firewall features that control network traffic are based on an extensible set of network service protocols, such as HTTP and SMTP. The Firebox Vclass appliances apply security policies defined by the management system to all incoming or outgoing traffic. Additional modules implement other security features, such as authentication, NAT, and QoS functions.

We use an open architectural structure to allow integration with common standards for network security. For example, our VPN component currently supports IPSec and IKE standards and the authentication module in our medium-large enterprise Firebox Vclass products support a variety of standard authentication methods.

Management features. Our management software allows a customer to manage and monitor the enterprise's Internet security with an intuitive, point-and-click user interface or Command Line Interface.

Integrated suite of system management tools. Our medium-large enterprise Firebox Vclass products use a Windows-based security management system that packages, configures and deploys security software, security policies and the operating system from the in-house manager's desktop computer to the enterprise's security appliances. The management system also includes logging and notification functions and real-time monitoring. Our management tools allow the management of multiple security appliances from a single location.

Because larger, distributed enterprise environments can be very different from single site deployments, we designed separate management systems for each. Our Firebox Vclass single appliance management software, Firebox Vcontroller, enables quick installation and management by an in-house manager using a standard Windows-based system. The WatchGuard CPM management software is designed specifically for ease of configuration and visual representation of a multiple appliance deployment. All management systems have the ability to remotely deploy new security software to the appliances or update their security engines from the management console.

Automated installation guides. Our automated installation guides enable enterprises to install and configure our Firebox Vclass products in as quickly as 15 to 30 minutes. Software updates or upgrades are also accessed through easy-to-use installation guides.

RapidStream “Secured by Check Point” Products

The RapidStream family of “Secured by Check Point” products are high-performance VPN and firewall appliances designed for customers ranging from mid-sized enterprises to Global 1000 companies. The RapidStream line of products, which is based on the same platform and similar hardened Linux-based operating system as our Firebox Vclass line of products, has similar hardware features but runs Check Point Next Generation, or NG, Firewall-1 and VPN-1 security software. This enables WatchGuard to address the specific needs of organizations that have standardized on Check Point software but need the high-performance hardware platform offered in the Firebox Vclass product line. RapidStream security appliances, which have passed Check Point certification, are also interoperable with over 300 complimentary solutions from OPSEC partners, Check Point’s open, multi-vendor security framework for the “best of breed” security approach traditionally favored by large enterprise end-users.

ServerLock System

For enterprises of all sizes, the ServerLock System provides server content and application security that protects critical data and services against unauthorized or unintentional access or manipulation. This protection is offered through a combination of kernel-level software, secured remote communications, centralized management and a simplified dual-mode administrative model. ServerLock represents a new model for protecting data, applications and the core of mission-critical systems by creating a new form of protection on the server.

System structure. The ServerLock System is comprised of the following components:

- *ServerLock.* Our ServerLock software resides on the protected server and acts as a filter between operations by the user and execution by the operating system. This protects the system against unauthorized or unintentional changes by even the most privileged user, the system administrator. Acting as a filter between requests for changes and the actual execution of those changes within the operating system kernel, ServerLock prevents changes to the operating system’s static components and the configurations that implement that server’s security policies.
- *ServerLock Manager.* Recognizing that users will implement ServerLock on multiple servers and, in large enterprises, on entire server farms, the ServerLock Manager is designed to maximize efficiency of control for tens and even hundreds of servers, all using secure, remote communication channels. The ServerLock Manager allows administrators or service providers to control multiple servers by applying custom rules and turning protection on and off in much the same manner as those tasks are performed locally. ServerLock’s remote communications channel is designed to simplify setting and resetting the protection state of remote machines and to make aggregating systems easier, which provides simplicity of depiction in a managed environment.
- *ServerLock console.* By allowing systems to be segregated into intuitive groupings by function, geography or any customer-selected criteria, the ServerLock console manages the protection state for all

managed servers with a simple click of a mouse. The ServerLock configuration interface is fully portable and may be run on remote administrator systems and laptops, thereby connecting security functions to the central management server.

- *Kernel-based protection.* Because all user-space processes, including authentication, are vulnerable to attack or accidental corruption by a privileged user or system administrator, ServerLock's protection, from filtering user requests to authenticating changes in the protection state, operates from the kernel. The kernel, which is the heart of the operating system, performs the most critical and fundamental system operations and represents the real core of any server. By applying ServerLock protection at this level, users are defended against virtually all attempts to corrupt systems. ServerLock also enables kernel-to-kernel remote communication using strong encryption implemented through a 239-bit elliptic curve cryptosystem adapted for ServerLock.
- *Simplified administration.* Internet security has historically been an area of complexity and confusion for enterprises. The security appliance, which was pioneered by WatchGuard, represents an important and groundbreaking development in simplification. By using a simplified dual-mode model for administering the security policy, ServerLock extends that simplification to maintaining the integrity of server content and applications. Critical resources are managed in two modes, operational and administrative. In operational mode, designated server content and applications are protected from unauthorized or unintentional access or manipulation. In administrative mode, standard, existing server protections are in force. ServerLock's simplified dual mode allows even a technically naive user to understand the protection: operational mode is in place when the business is operating and administrative mode is in place when the server needs to be administered.
- *Simplified installation.* Designed to complement the manner in which servers are built, configured and run, ServerLock's specialized license keys allow straightforward installation and require little discretion on the part of the installer.
- *Customizable protection.* For protection of specialized resources or applications, ServerLock provides a utility for creating and managing custom rules that can be used to protect individual files, proprietary applications or site-specific configuration parameters. This customizable protection is also managed with a simple on/off, operational/administrative protection model.

LiveSecurity Service. ServerLock customers also receive the benefits of our LiveSecurity Service. This includes access to technical support, software updates, threat responses, expert editorials, support flashes, virus alerts and interactive training.

AppLock/Web

Based on WatchGuard's ServerLock kernel protection, AppLock/Web specifically protects Microsoft NT/2000 IIS Web servers from both malicious and unintentional damage. This protection applies to the server operating system, the IIS application, and over 200 types of common content. This protection is offered through a combination of kernel-level software and a simplified dual-mode administrative model. Content protection is managed through a simple point-and-click customization interface.

System structure. AppLock/Web is comprised of the following components:

- *AppLock/Web.* Our AppLock/Web software resides on the protected server and acts as a filter between operations by the user and execution by the operating system. This protects the system against unauthorized or unintentional changes by even the most privileged user, the system administrator. Acting as a filter between requests for changes and the actual execution of those changes within the operating system kernel, AppLock/Web prevents changes to the operating system's static components and the configurations that implement that server's security policies. This protection is applied, and the content to be protected is discovered, automatically during the installation of the product.

- *AppLock/Web console.* Our AppLock/Web protections are managed with a local console that provides a simple interface to enable and disable protection, discover new content to protect, and provide protection to apply to new types of content not protected by default. The management of this protection is driven from a simple point-and-click system that allows users to select and sort at varying levels of granularity, from individual files to directories of files to specified file types.

LiveSecurity Service. AppLock/Web customers also receive the benefits of our LiveSecurity Service. This includes access to technical support, software updates, threat responses, expert editorials, support flashes, virus alerts and interactive training.

LiveSecurity Service

Our subscription-based LiveSecurity Service includes:

- *Information alerts.* Timely analyses of breaking Internet security news combined with instructions on how our customers can protect their systems.
- *Virus alerts.* Our strategic alliance with Network Associates, Inc. gives our customers real-time virus alerts from McAfee and specific information on how to protect their systems.
- *Threat responses.* Detailed information on high-profile security vulnerabilities as they develop, including information on how they may affect our customers' systems and what we are doing to help our customers keep their networks secure, and, when appropriate, software updates to address specific threats.
- *Software updates.* Customers receive on-going functional enhancements for their Firebox products or ServerLock/AppLock software on a when-and-if-available basis.
- *Support flashes.* Technical tutorials provide our customers with answers to frequently asked questions about managing WatchGuard products, in addition to information on new software updates.
- *Expert editorials.* The WatchGuard LiveSecurity Advisory Council, a network of top security consultants, offers its views on Internet security and provides a source of continuing education.
- *Technical support.* We provide subscribers with access to various levels of interactive and Web-based technical support.
- *Training.* We provide subscribers with access to interactive and Web-based product training and certification services.

Our scalable LiveSecurity Service, which runs on a collection of secured servers, registers subscribers, facilitates downloading our software to the desktop computers of registered subscribers and delivers LiveSecurity content to subscribers. To facilitate a high level of security and authenticity, we protect our servers with our own security system and strongly encrypt data communication between servers.

Managed Security Solution

WatchGuard's managed security solution for service providers has three main components: our network operations center, or NOC, security suite software with security and management features, our security appliances and our LiveSecurity Service.

Security features. Our managed security solution includes the same comprehensive set of security features offered in our Firebox products.

Management features. We designed our managed security solution management software for a trained operator using a dedicated management console to configure and manage the security of a large subscriber base. Centrally located at the service provider's NOC, our Global Policy Manager software provides security

intelligence and configuration for all customer sites under management. Our software allows the service provider to create and store various security policy configurations for different customer groups or service plans. For example, our service provider customers can choose to separately and remotely deploy select security features, such as VPN and Web blocking. This gives service providers the ability to incrementally add for-fee services to their basic service offering, without the expense of sending personnel to their customers' sites. To enable service providers to configure, monitor and manage the Internet security of thousands of customers, our managed security solution includes scalable logging and monitoring software called WatchGuard event processors. The event processors run on Sun Solaris-based workstations and can be located in the NOC or distributed at the service provider's point of presence. Each event processor manages the logging and notification features of up to 500 security appliances through commands issued from the Global Policy Manager at the NOC.

Security appliances. One or more of our security appliances reside on the premises of each managed customer of the service provider or are hosted in the service provider's data center. The appliances receive and implement the security software and security policies sent by the service provider. All of our security appliances may be centrally managed by the service provider.

LiveSecurity Service. Through our LiveSecurity Service, the service provider's NOC receives information and virus alerts, threat responses, software updates, support flashes and expert editorials, as well as access to training and service provider-specific technical support. The service provider then updates the security policies of its customers and transmits these policy updates over its network to its customers.

By receiving the benefits of our security solution through a service provider, an enterprise gains a number of added advantages. The service provider can:

- monitor and manage customers' security 24 hours a day, seven days a week;
- define and implement professional, customized Internet security policies;
- easily install software updates across its installed base;
- regularly review customers' security and provide detailed reporting and analysis; and
- mitigate the up-front cost of a security system purchase and setup.

Managed service providers, particularly those engaged in the fast-growing area of Web hosting, continue to vie for competitive advantage in their industry. With ServerLock, service providers can offer increased security for hosted content with only minimal incremental cost. ServerLock's management and deployment models enable lower cost of management and overhead through the same intuitive design that minimizes the administrative costs for an enterprise managing its own security.

Research and Development

We focus our research and development efforts on enhancing our existing products and services, developing new products based on our innovative distributed-appliance architecture, developing new high-performance ASIC technology and developing services that capitalize on our LiveSecurity Service infrastructure. We use a modular design, which allows us to develop new applications that plug into our existing product line. As a result, our products can be deployed in stages, either directly by an enterprise or by a service provider if the enterprise has outsourced its security management. As we develop new products, our LiveSecurity Service end-users and service provider partners can incorporate the new products and services into their systems with minimal system interruption.

As of December 31, 2002, we employed 118 people on our research and development staff. Research and development expenses were \$13.9 million in 2000, \$18.9 million in 2001 and \$20.9 million in 2002. We have product development facilities in Seattle, Washington, San Jose and Tustin, California and Waltham, Massachusetts.

Competition

We compete in a market that is intensely competitive, highly fragmented and rapidly changing. We face competition in sales both of products and services designed for enterprises and those designed for service providers. We have experienced and will continue to experience increasing competition from current and emerging competitors, many of which have significantly greater financial, technical, marketing and other resources than we do.

In the market for Internet security solutions, we compete on the basis of technological expertise and functionality, breadth of service and product technology and features, ease of installation and management, performance, updatability, scalability, brand recognition, price, customer support and distribution capability. Currently, the primary competitors in our industry include Check Point, Cisco Systems, Inc., Netscreen Technologies, Inc., Nokia Corporation, SonicWALL, Inc. and Symantec Corporation. Other competitors offering security products include hardware and software vendors such as Lucent Technologies, Inc. and Network Associates, Inc., operating system vendors such as Microsoft Corporation, Novell, Inc. and Sun Microsystems, Inc., and a number of smaller companies.

Our competitors may be able to respond more quickly to new or emerging technologies and changes in customer requirements than we can. In addition, our current and future competitors may bundle their products with other software or hardware, including operating systems and browsers, in a manner that may discourage users from purchasing the products and services we offer. Many of our current and potential competitors have greater name recognition, larger customer bases to leverage and greater access to proprietary technology, and could therefore gain market share to our detriment. In addition, our current and potential competitors may establish cooperative relationships among themselves or with third parties that may further enhance their resources, such as the relationship between Check Point and Nokia. We expect additional competition as other established and emerging companies enter the Internet security market and new products and technologies are introduced.

While some of our competitors have traditionally targeted large-enterprise security needs, these vendors could adapt their existing products to make them more attractive to our markets. If these or other of our competitors were to focus their greater financial, technical and marketing resources on our markets, our business could be harmed. In addition, as our security solutions are adopted by larger enterprises, we expect to see increased competition. Increased competition in any of our markets could result in price reductions, fewer customer orders, reduced gross margins and loss of market share.

Proprietary Rights

To protect our proprietary rights, we rely primarily on

- copyright, trademark, service mark and trade secret laws;
- license agreements with third parties, including a standard software license included with our products;
- confidentiality agreements with our employees and third parties;
- invention assignment agreements with our employees and contractors;
- protective contractual provisions in our agreements with some of our consultants, resellers and customers; and
- limited access to our software, documentation and other proprietary information.

The following are trademarks of ours or our affiliates: WatchGuard® is a registered trademark in the United States, the European Union, Canada, Norway, Australia, New Zealand, Indonesia, Singapore and Japan, RapidStream® is a registered trademark in the United States and South Korea, Designing Peace of Mind® is a registered trademark in the United States, the WatchGuard logo is a registered trademark in the United States, LiveSecurity® is a registered trademark in the United States, the European Union, Canada and Mexico, Firebox® is a registered trademark in the United States, RapidCore® is a registered trademark in the United States, the European Union and Japan, ServerLock® is a registered trademark in the United States, Australia, Japan, Norway

and Singapore, AppLock® is a registered trademark in the United States and LockSolid® is a registered trademark in the United States, Australia, Japan, New Zealand and Norway. Applications to register the WatchGuard, RapidStream, LiveSecurity, Firebox, RapidCore, ServerLock and LockSolid trademarks are pending in other jurisdictions. We also have other trademarks in use in the United States that do not currently have applications pending in any jurisdiction. Check Point, Firewall-1 and VPN-1 are either trademarks, service marks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. We have one issued patent and 20 patents pending.

Many of our products are designed to include software or other intellectual property licensed from third parties. While it may be necessary in the future to seek or renew licenses relating to various aspects of our products, we believe, based on past experience and standard industry practice, that such licenses generally could be obtained on commercially reasonable terms. Nonetheless, the necessary licenses may not be available on acceptable terms, if at all. Our inability to obtain certain licenses or other rights or to obtain such licenses or rights on favorable terms, or the need to engage in litigation regarding these matters, could have a material adverse effect on our business, financial condition and operating results. Moreover, inclusion in our products of software or other intellectual property licensed from third parties on a non-exclusive basis can limit our ability to protect our proprietary rights in our products.

U.S. Government Export Regulation Compliance

Our products are subject to U.S. governmental regulations governing the export of encryption commodities and software. In recent years, however, U.S. legislation has relaxed export controls on encryption. U.S. law now allows the export of encryption commodities and software of any strength to nongovernmental end-users located in any country except those designated as embargoed or otherwise restricted by the U.S. government, subject to streamlined reporting requirements. To satisfy these encryption export reporting requirements, we use data gathered from end-users during product registration. WatchGuard's encryption commodities and software have been approved for export by the U.S. Department of Commerce's Bureau of Industry and Security, or BIS, under an export license exception granted after previous technical reviews by the BIS. The approved commodities and software include our branch office and remote user VPN software and our Firebox II, Firebox III, Firebox Vclass and RapidStream "Secured by Check Point" lines of security appliances. The BIS has granted retail export status to our Firebox 700, Firebox V10 and Firebox SOHO security appliances, which use encryption in branch office VPN software. We are eligible to export products that qualify for retail export status to all nonembargoed and nonrestricted foreign end-users, including government entities.

Manufacturing

We currently outsource all hardware manufacturing and assembly for certain of our security appliances for SMEs and larger enterprises to Washington-based ETMA Corporation, our primary supplier, with Malaysia-based Unico Technology Berhad (an affiliate of ETMA Corporation) as our back-up supplier. For certain of our larger enterprise products, we outsource the board assembly to San Jose-based Alta Manufacturing Inc. For the remainder of our security appliances for SMEs and larger enterprises, we outsource all hardware manufacturing to Minnesota-based Repron Electronic Inc. Our contract manufacturer for our Firebox SOHO security appliances is Sercomm Corporation, a Taiwan, Republic of China-based corporation. All contract manufacturers are certified as meeting the International Organization for Standardization's quality assurance standards ISO 9001 and 9002. We are currently reviewing other contract manufacturers for potential engagement as either primary or back-up suppliers for current and future products. Worldwide distribution is currently performed at our distribution facility in Seattle, Washington.

Employees

As of December 31, 2002, we had 331 employees. Of these, 117 were employed in sales and marketing, 38 in finance and administration, 58 in customer support and operations and 118 in research and development. We are not a party to any collective bargaining agreements with our employees and we have not experienced any work stoppages. We believe we have good relations with our employees.

IMPORTANT FACTORS THAT MAY AFFECT OUR OPERATING RESULTS, OUR BUSINESS AND OUR STOCK PRICE

In addition to the other information contained in this annual report, you should carefully read and consider the following risk factors. If any of these risks actually occur, our business, financial condition or operating results could be adversely affected and the trading price of our common stock could decline.

We have incurred losses in the past and may not achieve or sustain consistent profitability, which could result in a decline in the value of our common stock.

Since inception, we have incurred net losses and experienced negative cash flows from operations in each quarter, except that we had net income and a positive cash flow from operations in the third quarter of 2000 and a positive cash flow from operations in the third quarter of 2001. As of December 31, 2002, we had an accumulated deficit of approximately \$114 million. Although our revenues have increased each year since we began operations, we do not believe that the historical percentage growth rate of our revenues will be sustainable as our revenue base increases and we may not achieve or sustain profitability in future periods. We expect that over time we will have to increase our operating expenses in connection with

- continuing to develop our technology;
- expanding into new product markets;
- expanding into new geographic markets;
- pursuing additional strategic acquisitions;
- hiring additional personnel; and
- upgrading our information and internal control systems.

If we are unable to achieve or sustain profitability in future quarters, the trading price of our common stock could decline.

Our operating results fluctuate and could fall below expectations of securities analysts and investors, resulting in a decline in our stock price.

Our quarterly and yearly operating results have varied widely in the past and will probably continue to fluctuate. For this reason, we believe that period-to-period comparisons of our operating results may not be meaningful. In addition, our limited operating history makes predicting our future performance difficult. If our operating results for a future quarter or year fail to meet market expectations, this shortfall could result in a decline in our stock price.

The economic downturn in the U.S. economy has adversely affected the demand for our products and services and may continue to result in decreased revenue and growth rates. We do not know how long this economic downturn will last or how severe it will become. We also cannot predict the extent of the effect of the economic downturn in the United States on economies in other countries and geographic regions in which we conduct business. To the extent that this downturn continues or grows deeper in the United States or other geographic regions in which we operate, the Internet security industry and demand for our products and services are likely to be adversely affected.

We base our spending levels for product development, sales and marketing and other operating expenses largely on our expected future revenues. Because our expenses are largely fixed for a particular quarter or year, we may be unable to adjust our spending in time to compensate for any unexpected quarterly or annual shortfall in revenues. A failure to so adjust our spending in time also could cause operating results to fall below the expectations of securities analysts and investors, resulting in a decline in our stock price.

If our estimates or judgments relating to our critical accounting policies are based on assumptions that change or prove to be incorrect, our operating results could fall below expectations of securities analysts and investors, resulting in a decline in our stock price.

Our discussion and analysis of financial condition and results of operations in this annual report is based on our consolidated financial statements, which have been prepared in accordance with accounting principles generally accepted in the United States. The preparation of financial statements in conformity with generally accepted accounting principles requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. On an ongoing basis, we evaluate significant estimates used in preparing our consolidated financial statements, including those related to:

- revenue recognition, including sales returns and allowances;
- bad debt;
- inventory reserves;
- restructuring reserves; and
- analysis of impairment of goodwill and other long-lived intangible assets.

We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as provided in our discussion and analysis of financial condition and results of operations in this annual report, the results of which form the basis for making judgments about the carrying values of assets and liabilities that are not readily apparent from other sources. Examples of such estimates include, but are not limited to, those associated with the costs of our 2001 and 2002 restructuring and impairment analysis of our Qiave intangible asset, as well as goodwill relating to the acquisitions of BeadleNet, Qiave and RapidStream. Although we do not anticipate further significant adjustments to our 2002 restructuring, the actual costs related to the restructuring may differ from estimate if it takes us longer than expected to find suitable tenants or if there are further changes in the real estate market where excess facilities are located. Actual results may differ from these and other estimates if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our operating results to fall below the expectations of securities analysts and investors, resulting in a decline in our stock price.

Because many potential customers do not fully understand or remain unaware of the need for comprehensive Internet security or may perceive it as costly and difficult to implement, our products and services may not achieve market acceptance.

We believe that many potential customers, particularly SMEs, do not fully understand or are not aware of the need for comprehensive Internet security products and services, particularly those products designed for server content and application security. Historically, only enterprises having substantial resources have developed or purchased comprehensive Internet security solutions. Also, there is a perception that comprehensive Internet security is costly and difficult to implement. We will therefore not succeed unless the market understands the need for comprehensive Internet security and we can convince our potential customers of our ability to provide this security in a cost-effective and administratively feasible manner. Although we have spent, and will continue to spend, considerable resources educating potential customers about the need for comprehensive Internet security and the benefits of our products and services, our efforts may be unsuccessful.

If potential customers do not accept our Firebox products and the related LiveSecurity Service, our business will not succeed.

We currently expect that future revenues will be primarily generated through sales of our Firebox products and the related LiveSecurity Service, including subscription fees, and we cannot succeed if the market does not accept these products and services. Our success depends on our ability and the ability of our distribution network, which includes distributors, VARs and Internet service providers and other managed service providers, to obtain and retain customers. Some of our Firebox products, particularly the Firebox Vclass products based on the

RapidStream technology we acquired in the second quarter of 2002, however, are relatively new and unproven. The Firebox Vclass products were launched in May 2002 and delivered in June 2002, and the broadcast portion of our LiveSecurity Service has been available only since February 1999. The Firebox Vclass products are also directed at a new class of customer for us, one that requires a high-performance security solution with enterprise-level networking functionality and VPN scalability, and we may be unsuccessful in marketing and selling to this class of customer.

To receive our LiveSecurity Service, enterprises are required to pay an annual subscription fee, either to us or, if they obtain the LiveSecurity Service through one of our channel customers, to the channel customer. We are not aware of any other Internet security product that allows enterprises to keep their security solution current by receiving software updates and comprehensive security information over the Internet. Enterprises may be unwilling to pay a subscription fee to keep their Internet security up to date and to receive Internet security-related information. Because our LiveSecurity Service is an innovative service, we may not be able to accurately predict the rate at which our customers will renew their annual subscriptions. In addition, most businesses implementing security services have traditionally managed their own Internet security rather than using the services of third-party service providers. As a result, our products and services and the outsourcing of Internet security to third parties may not achieve significant market acceptance.

We may not realize any significant benefits from our relationship with Check Point Software Technologies Ltd. or the sale of the RapidStream-branded "Secured by Check Point" line of products.

Following our acquisition of RapidStream in the second quarter of 2002, we entered into a relationship with Check Point under which we market a line of products that includes Check Point security software. These products, which are sold under the RapidStream brand as "Secured by Check Point," are new and unproven and may not achieve market acceptance. In addition, Check Point is a competitor of ours in the Internet security industry, and our relationship with Check Point is terminable by either party at will. If Check Point discontinues its relationship with us or fails to devote sufficient resources and attention to the marketing of our RapidStream products, we may not realize any benefits from our relationship with Check Point and may not generate significant revenues from the sale of the RapidStream line of products.

If we are unable to compete successfully in the highly competitive market for Internet security products and services, our business will fail.

The market for Internet security products is intensely competitive and we expect competition to intensify in the future, particularly with our expansion into the larger enterprise market with our products based on RapidStream technology. An increase in competitive pressures in our market or our failure to compete effectively may result in pricing reductions, reduced gross margins and loss of market share. Currently, the primary competitors in our industry include Check Point, Cisco Systems, Inc., NetScreen Technologies, Inc., Nokia Corporation, SonicWALL, Inc. and Symantec Corporation. Other competitors offering security products include hardware and software vendors such as Lucent Technologies, Inc. and Network Associates, Inc., operating system vendors such as Microsoft Corporation, Novell, Inc. and Sun Microsystems, Inc., and a number of smaller companies. Many of our competitors have longer operating histories, greater name recognition, larger customer bases and significantly greater financial, technical, marketing and other resources than we do. In addition, our current and potential competitors may establish cooperative relationships among themselves or with third parties that may further enhance their resources. As a result, they may be able to adapt more quickly to new technologies and customer needs, devote greater resources to the promotion or sale of their products and services, initiate or withstand substantial price competition, take advantage of acquisition or other opportunities more readily or develop and expand their product and service offerings more quickly. In addition, our competitors may bundle products competitive with ours with other products that they may sell to our current or potential customers. These customers may accept these bundled products rather than separately purchasing our products.

If our third-party channel customers fail to perform, our ability to sell our products and services will be limited.

We sell most of our products and services through our distribution network, and we expect our success to continue to depend in large part on the performance of this network. Our channel customers have the ability to sell products and services that are competitive with ours, to devote more resources to those competitive products or to cease selling our products and services altogether. Two of our channel customers, Ingram Micro and Tech Data, together accounted for 26% of our revenues in the year ended December 31, 2002. The loss of one of these distributors, a reduction in their sales, a reduction in our share of their sales of Internet security products, or a loss or reduction in sales involving one or more other channel customers, particularly if the reduction results in increased sales of competitive products, could harm our business. In addition, we are in the process of consolidating our channel by reducing the number of channel customers with whom we have a direct contract, while expanding our programs for our indirect partners to improve overall performance and efficiencies. While we have made progress in the Americas and Europe/Middle East/Africa regions, we are in an earlier stage of that process in the Asia Pacific region where, in addition to consolidation, a channel reorganization is required. If this consolidation and reorganization causes disruption, we could experience a loss or reduction in sales involving one or more of our channel customers.

Product returns, retroactive price adjustments and rebates could exceed our allowances, which could adversely affect our operating results.

We provide most of our channel customers with product return rights for stock rotation and price protection rights for their inventories, which they may exercise if we lower our prices for those products. We also provide promotional rebates to some of our channel customers. We may experience significant returns, price adjustments and rebate costs for which we may not have adequate allowances. The short life cycles of our products and the difficulty of predicting future sales increase the risk that new product introductions or price reductions by us or our competitors could result in significant product returns or price adjustments. When we introduced the Firebox II, and then later the Firebox III, security appliances, we experienced an increase in returns of previous products and product versions. Provisions for returns and allowances were \$1.9 million in 2000, \$6.9 million in 2001 and \$4.6 million in 2002 or 3%, 10% and 6% of total revenues before returns and allowances. While we review and adjust our provision for returns and allowances in order to properly reflect the potential for promotional rebate costs, increased returns and pricing adjustments associated with new products, including new products resulting from our acquisition of RapidStream, the provision may still be inadequate.

Rapid changes in technology and industry standards could render our products and services unmarketable or obsolete, and we may be unable to introduce new products and services timely and successfully.

To succeed, we must continually change and improve our products in response to rapid technological developments and changes in operating systems, Internet access and communications, application and networking software, computer and communications hardware, programming tools, computer language technology and hacker techniques. We may be unable to successfully and timely develop these new products and services or achieve and maintain market acceptance. The development of new, technologically advanced products and services is a complex and uncertain process that requires great innovation and the ability to anticipate technological and market trends. Because Internet security technology is complex, it can require long development and testing periods.

Releasing new products and services prematurely may result in quality problems, and releasing them late may result in loss of customer confidence and market share. In the past, we have on occasion experienced delays in the scheduled introduction of new and enhanced products and services, and we may experience delays in the future. When we do introduce new or enhanced products and services, we may be unable to successfully manage the transition from the older products and services to minimize disruption in customer ordering patterns, avoid excessive inventories of older products and deliver enough new products and services to meet customer demand.

Seasonality and concentration of revenues at the end of the quarter could cause our revenues to fall below the expectations of securities analysts and investors, resulting in a decline in our stock price.

The growth rate of our domestic and international sales has been and may in the future be lower in the summer months, when businesses often defer purchasing decisions. Also, as a result of customer buying patterns and the efforts of our sales force to meet or exceed quarterly and year-end quotas, historically we have received a substantial portion of a quarter's sales orders and earned a substantial portion of a quarter's revenues during the quarter's last month and the latter half of the last month. If expected revenues at the end of any quarter are delayed, our revenues for that quarter could fall below the expectations of securities analysts and investors, resulting in a decline in our stock price.

We may be unable to adequately expand our operational systems to accommodate growth, which could harm our ability to deliver our products and services.

Our operational systems have not been tested at the customer volumes that may be required in the future. We may encounter performance difficulties when operating with a substantially greater number of customers. These performance difficulties could harm our ability to deliver our products and services. An inability to add software and hardware or to develop and upgrade existing technology or operational systems to handle increased traffic may cause unanticipated system disruptions, slower response times and poor customer service, including problems filling customer orders.

We may be required to defend lawsuits or pay damages in connection with the alleged or actual failure of our products and services.

Because our products and services provide and monitor Internet security and may protect valuable information, we may face claims for product liability, tort or breach of warranty relating to our products and services. Anyone who circumvents our security measures could misappropriate the confidential information or other property of end-users using our products and services or interrupt their operations. If that happens, affected end-users or channel customers may sue us. In addition, we may face liability for breaches caused by faulty installation and implementation of our products by end-users or channel customers. Although we attempt to reduce the risk of losses from claims through contractual warranty disclaimers and liability limitations, these provisions may be unenforceable. Some courts, for example, have found contractual limitations of liability in standard software licenses to be unenforceable because the licensee does not sign the license. Defending a suit, regardless of its merit, could be costly and could divert management attention. Although we currently maintain business liability insurance, this coverage may be inadequate or may be unavailable in the future on acceptable terms, if at all.

A breach of security could harm public perception of our products and services.

We will not succeed unless the marketplace is confident that we provide effective Internet security protection. Even networks protected by our software products may be vulnerable to electronic break-ins and computer viruses. If an actual or perceived breach of Internet security occurs in an end-user's systems, regardless of whether the breach is attributable to us, the market perception of the efficacy of our products and services could be harmed. This could cause us or our channel customers to lose current and potential customers or cause us to lose potential channel customers. Because the techniques used by computer hackers to access or sabotage networks change frequently and generally are not recognized until launched against a target, we may be unable to anticipate these techniques.

If we are unable to prevent attacks on our internal network system by computer hackers, public perception of our products and services will be harmed.

Because we provide Internet security, we are a significant target of computer hackers. We have experienced attacks by computer hackers in the past and expect attacks to continue. If attacks on our internal network system are successful, public perception of our products and services will be harmed.

We may be unable to adequately protect our operational systems from damage, failure or interruption, which could harm our reputation and our ability to attract and retain customers.

Our operations, customer service, reputation and ability to attract and retain customers depend on the uninterrupted operation of our operational systems. Although we utilize limited off-site backup facilities and take other precautions to prevent damage, failure or interruption of our systems, our precautions may be inadequate. Any damage, failure or interruption of our computer or communications systems could lead to service interruptions, delays, loss of data and inability to accept and fill customer orders and provide customers with our LiveSecurity Service.

We may be unable to deliver our products and services if we cannot continue to license third-party technology that is important for the functionality of our products.

Our success will depend in part on our continued ability to license technology that is important for the functionality of our products. A significant interruption in the supply of a third-party technology could delay our development and sales until we can find, license and integrate equivalent technology. This could damage our brand and result in loss of current and potential customers. Although we believe that we could find other sources for the technology we license, alternative technologies may be unavailable on acceptable terms, if at all. We depend on our third-party licensors to deliver reliable, high-quality products, develop new products on a timely and cost-effective basis and respond to evolving technology and changes in industry standards. We also depend on the continued compatibility of our third-party software with future versions of our products.

We may be unable to deliver our products and services if component manufacturers fail to supply component parts with acceptable quantity, quality and cost.

We obtain the component parts for our hardware from a variety of manufacturers. While our component vendors have produced parts for us in acceptable quantities and with acceptable quality and cost in the past, they may be unable to do so in the future. Companies in the electronics industry regularly experience lower-than-required component allocations, and the industry is subject to frequent component shortfalls. Although we believe that we could find additional or replacement sources for our hardware components, our operations could be disrupted if we have to add or switch to a replacement vendor or if our component supply is interrupted for an extended period. This could result in loss of customer orders and revenue.

Governmental controls over the export or import of encryption technology could cause us to lose sales.

Any additional governmental regulation of imports or exports or failure to obtain required export approval of our encryption technologies could adversely affect our international and domestic sales. The United States and various other countries have imposed controls, export license requirements and restrictions on the import or export of some technologies, especially encryption technology. In addition, from time to time governmental agencies have proposed additional regulation of encryption technology, such as requiring the escrow and governmental recovery of private encryption keys. Additional regulation of encryption technology could delay or prevent the acceptance and use of encryption products and public networks for secure communications. This, in turn, could result in decreased demand for our products and services. In addition, some foreign competitors are subject to less stringent controls on exporting their encryption technologies. As a result, they may be able to compete more effectively than we can in the U.S. and international Internet security markets.

We may be unable to adequately protect our proprietary rights, which may limit our ability to compete effectively.

Despite our efforts to protect our proprietary rights, unauthorized parties may misappropriate or infringe on our trade secrets, copyrights, trademarks, service marks and similar proprietary rights. We face additional risk when conducting business in countries that have poorly developed or inadequately enforced intellectual property laws. While we are unable to determine the extent to which piracy of our software products exists, we expect piracy to be a continuing concern, particularly in international markets and as a result of the growing use of the Internet.

If we fail to obtain and maintain patent protection for our technology, we may be unable to compete effectively. We have one issued patent and 20 patents pending, but our patent applications may not result in issued patents. Even if we secure a patent, the patent may not provide meaningful protection. In addition, we rely on unpatented proprietary technology. Because this proprietary technology does not have patent protection, we may be unable to meaningfully protect this technology from unauthorized use or misappropriation by a third party. In addition, our competitors may independently develop similar or superior technologies or duplicate any unpatented technologies that we have developed, which could significantly reduce the value of our proprietary technology or threaten our market position.

Intellectual property claims and litigation could subject us to significant liability for damages and invalidation of our proprietary rights.

In the future, we may have to resort to litigation to protect our intellectual property rights, to protect our trade secrets or to determine the validity and scope of the proprietary rights of others. Any litigation, regardless of its success, would probably be costly and require significant time and attention of our key management and technical personnel. Litigation could also force us to

- stop or delay selling, incorporating or using products that incorporate the challenged intellectual property;
- pay damages;
- enter into licensing or royalty agreements, which may be unavailable on acceptable terms; or
- redesign products or services that incorporate infringing technology.

Although we have not been sued for intellectual property infringement, we may face infringement claims from third parties in the future. The software industry has seen frequent litigation over intellectual property rights, and we expect that participants in the Internet security industry will be increasingly subject to infringement claims as the number of products, services and competitors grows and functionality of products and services overlaps.

Undetected product errors or defects could result in loss of revenues, delayed market acceptance and claims against us.

Our products and services may contain undetected errors or defects, especially when first released. Despite extensive testing, some errors are discovered only after a product has been installed and used by customers. Any errors discovered after commercial release could result in loss of revenues or claims against us or our channel customers.

If we do not retain our key employees, our ability to execute our business strategy will be impaired.

Our future success will depend largely on the efforts and abilities of our senior management and our key development, technical, operations, information systems, customer support and sales and marketing personnel, and on our ability to retain them. These employees are not obligated to continue their employment with us and may leave us at any time.

In attempting to integrate the business and technology of any future acquisition, we could incur significant costs that may not be outweighed by any benefits of the acquisition.

As part of our business strategy, we may acquire other companies, products or technologies, and these acquisitions may result in substantial costs. The costs of any future acquisitions may include costs for:

- integration of operations, including combining teams and processes in various functional areas;
- reorganization or closure of operations and facilities;

- integration of new technology into our products;
- fees and expenses of professionals involved in completing the integration process; and
- potential existing liabilities of any future acquisition target.

Successful integration of the operations, technology, products, customers, suppliers and personnel of any future acquisition could place a significant burden on our management and internal resources. The diversion of the attention of our management and any difficulties encountered in the transition and integration process could disrupt our business and have an adverse effect on our business and operating results.

If we do not expand our international operations and successfully overcome the risks inherent in international business activities, the growth of our business will be limited.

Our ability to grow will depend in part on the expansion of our international sales and operations, which are expected to continue to account for a significant portion of our revenues. Sales to customers outside of the United States accounted for approximately 55% of total revenues in 2000, 56% in 2001 and 58% in 2002. The failure of our channel customers to sell our products internationally would limit our ability to increase our revenues. In addition, our international sales are subject to the risks inherent in international business activities, including

- cost of customizing products for foreign countries;
- export and import restrictions, such as those affecting encryption commodities and software or those requiring local content;
- difficulties in acquiring and authenticating customer information;
- reduced protection of intellectual property rights and increased liability exposure; and
- regional economic and political conditions.

Our international sales currently are U.S. dollar-denominated. As a result, an increase in the value of the U.S. dollar relative to foreign currencies has made and may continue to make our products less competitive in international markets.

We may need additional capital and our ability to secure additional funding is uncertain.

Our future revenues may be insufficient to support the expenses of our operations and the expansion of our business. We may therefore need additional equity or debt capital. We may seek additional funding through

- public or private equity financings, which could result in significant dilution to stockholders;
- public or private debt financings; and
- capital lease transactions.

We believe that existing cash and cash equivalent balances will be sufficient to meet our capital requirements for at least the next 12 months. Our capital requirements will depend on several factors, however, including

- the rate of market acceptance of our products and services;
- our ability to expand our customer base;
- the growth of our sales and marketing capabilities; and
- the cost of any acquisitions we may complete.

Financing may be unavailable to us when needed or on acceptable terms.

Our stock price is volatile.

The trading price of our common stock could be subject to fluctuations for a number of reasons, including

- actual or anticipated variations in quarterly or annual operating results;
- changes in analysts' earnings projections or recommendations;
- failure to meet analysts' revenue or earnings projections;

- inability to successfully implement our business strategy;
- changes in business conditions affecting our customers, our competitors and us; and
- changes in accounting standards that adversely affect our revenues and earnings.

In recent years, moreover, the stock market in general and the market for Internet-related technology companies in particular have experienced extreme price and volume fluctuations, often unrelated to the operating performance of the affected companies. Our common stock has experienced, and is likely to continue to experience, these fluctuations in price, regardless of our performance.

ITEM 2. PROPERTIES

Our principal administrative, marketing, sales, development and operations facility is located in Seattle, Washington. We occupy approximately 100,000 square feet in this facility (including space that is subleased) under a lease that expires in September 2010. We have the option to extend the lease for an additional five-year term. We also maintain a product fulfillment and distribution warehouse in Seattle under a lease that expires in April 2006. In addition, we maintain offices in San Jose and Tustin, California and Waltham, Massachusetts. Our excess facilities at our corporate headquarters in Seattle, and in Aliso Viejo and San Jose, California, are partially subleased to tenants, with sublease terms that expire between 2003 and 2007.

ITEM 3. LEGAL PROCEEDINGS

We are not currently a party to any material legal proceedings.

ITEM 4. SUBMISSION OF MATTERS TO A VOTE OF SECURITY HOLDERS

No matters were submitted to a vote of our security holders during the fourth quarter of 2002.

PART II

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY AND RELATED STOCKHOLDER MATTERS

Market Information

Our common stock began trading on the Nasdaq National Market on July 30, 1999 under the symbol WGRD. The following table lists, for the periods indicated, the high and low sales prices per share of our common stock as reported on the Nasdaq National Market.

	Price Range of Common Stock	
	High	Low
Year Ended December 31, 2001		
First quarter	\$32.00	\$6.00
Second quarter	10.50	5.00
Third quarter	13.90	6.72
Fourth quarter	12.99	6.02
Year Ended December 31, 2002		
First quarter	8.08	4.90
Second quarter	6.71	4.35
Third quarter	5.65	4.05
Fourth quarter	6.95	3.03

The last reported sale price of our common stock on the Nasdaq National Market on March 17, 2002 was \$5.00 per share.

Holder

As of March 17, 2003, there were approximately 175 holders of record of our common stock. This does not include the number of persons whose stock is held in nominee or "street name" through brokers or other fiduciaries.

Dividends

We have never paid cash dividends on our common stock. We currently intend to retain any future earnings to fund the development and growth of our business and therefore do not anticipate paying any cash dividends in the foreseeable future.

Recent Sales of Unregistered Securities

None.

ITEM 6. SELECTED FINANCIAL DATA

When you read this selected financial data, it is important that you also read the historical consolidated financial statements and related notes included in this annual report, as well as the section entitled "Management's Discussion and Analysis of Financial Condition and Results of Operations." The historical results are not necessarily indicative of future results.

	Year Ended December 31,				
	1998	1999	2000	2001	2002
	(In thousands, except per share data)				
Consolidated Statement of Operations Data:					
Revenues:					
Product	\$10,678	\$ 17,329	\$ 52,010	\$ 46,893	\$ 53,200
Service	701	3,290	8,693	17,390	22,300
Total revenues	11,379	20,619	60,703	64,283	75,500
Cost of revenues:					
Product	3,653	6,954	18,932	20,658	19,888
Service	272	1,010	2,987	5,824	5,969
Total cost of revenues	3,925	7,964	21,919	26,482	25,857
Gross margin	7,454	12,655	38,784	37,801	49,643
Operating expenses:					
Sales and marketing	8,519	13,512	24,213	29,717	33,693
Research and development	4,442	7,118	13,900	18,854	20,858
General and administrative	2,454	3,646	6,001	7,726	7,804
Stock-based compensation	1,039	926	8,407	9,433	1,450
Amortization of goodwill	—	155	1,005	7,347	—
Amortization and impairment of other intangible assets acquired	—	90	2,823	3,595	11,055
Acquired in-process technology	—	3,381	4,399	—	1,179
Restructuring charges	—	—	—	3,720	8,091
Total operating expenses	16,454	28,828	60,748	80,392	84,130
Operating loss	(9,000)	(16,173)	(21,964)	(42,591)	(34,487)
Interest income (expense), net	(119)	155	6,515	5,771	2,920
Loss before income taxes	(9,119)	(16,018)	(15,449)	(36,820)	(31,567)
Provision for income taxes	—	—	215	157	29
Net loss	<u>\$ (9,119)</u>	<u>\$ (16,018)</u>	<u>\$ (15,664)</u>	<u>\$ (36,977)</u>	<u>\$ (31,596)</u>
Basic and diluted net loss per share (1)	<u>\$ (11.34)</u>	<u>\$ (1.80)</u>	<u>\$ (0.66)</u>	<u>\$ (1.38)</u>	<u>\$ (1.02)</u>
Shares used in calculation of basic and diluted net loss per share (1)	<u>804</u>	<u>8,903</u>	<u>23,556</u>	<u>26,723</u>	<u>31,029</u>

(1) See Notes 1 and 6 of the notes to our consolidated financial statements for an explanation of the method used to calculate basic and diluted net loss per share.

	December 31,				
	1998	1999	2000	2001	2002
	(In thousands)				
Consolidated Balance Sheet Data:					
Cash, cash equivalents and short-term investments	\$1,712	\$26,401	\$115,115	\$113,743	\$ 89,302
Deferred revenues	1,841	4,233	11,874	15,709	18,451
Long-term debt	—	—	—	—	—
Working capital	(274)	24,395	117,065	103,792	69,458
Total assets	9,032	41,311	195,930	173,031	189,298
Total stockholders' equity	881	32,245	172,405	148,304	151,764
Dividends payable	—	—	—	—	—

ITEM 7: MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

Overview

WatchGuard is a leading provider of Internet security solutions designed to protect enterprises that use the Internet for e-commerce and secure communications. Our award-winning products and services include our high-performance Firebox and RapidStream firewall and VPN appliances for access control, secure communications and (with certain of our Firebox products) network-based intrusion protection capabilities, and our ServerLock technology and anti-virus solution for content and application security for servers and desktops with host-based intrusion protection capabilities. Our innovative subscription-based LiveSecurity Service delivers threat responses, software updates, expert editorials, support flashes and virus alerts, which enables our customers, with minimal effort, to protect their data and communications in a continuously changing environment. Our core market spans the small- to medium-sized enterprise, or SME, market, from companies at the lower end where ease-of-use is a key requirement, to companies at the high end, including those with high-speed connections supporting VPNs between the corporate headquarters and geographically dispersed branch offices, where performance, scalability and networking features are key requirements. In addition, with the recent addition of our RapidStream line of "Secured by Check Point" appliances, we also have the opportunity to leverage the established presence of Check Point Software Technologies Ltd., or Check Point, in the large enterprise market.

Since our inception, we have invested heavily in the development of our products as follows:

- In September 1996, we introduced our initial Firebox security appliance and began selling our products both domestically and internationally.
- In 1998, we launched our managed security solution for Internet service providers and other managed service providers and introduced our second-generation Firebox II security appliances, which added significant functionality to our existing product lines.
- In February 1999, we launched the broadcast portion of our LiveSecurity Service.
- In October 1999, we acquired BeadleNet, LLC, a developer of Internet security solutions for small offices and home offices, or SOHOs.
- In the first quarter of 2000, we began shipping our security solutions for SOHOs and telecommuters.
- In October 2000, we acquired Qiave Technologies Corporation, a developer of digital information security systems. The acquisition allowed us to expand our product line with ServerLock, which protects server content and applications against unauthorized or unintentional changes.
- In February 2001, we announced the introduction of our ServerLock for NT products, which we began shipping in the first quarter of 2001.
- During the second and third quarters of 2001, we introduced a product line based on a higher-performance, third-generation security appliance, our Firebox III, including products targeted at the middle to lower-end of the SME market and small businesses and branch offices.
- In April 2002, we acquired RapidStream, Inc., a privately held provider of high-performance, ASIC (application-specific integrated circuit)-based firewall and VPN appliances.
- In April 2002, we entered into a partnership with Check Point to deliver a RapidStream "Secured by Check Point" line of high-performance security firewall and VPN appliances based on Check Point's custom-designed security ASIC technology and integrating Check Point NG software, which is targeted at the Global 1000 and large enterprise market. In July 2002, we introduced this RapidStream line.
- In the second quarter of 2002, we introduced high-performance Firebox Vclass VPN and firewall appliances, which are based on custom-designed security ASIC processors and are designed to address the performance and flexibility needs of a wide range of customers, including those in the higher end of the SME market that are running large distributed networks and data center environments.

- In August 2002, we introduced our new Firebox SOHO 6, Firebox SOHO 6tc, and Firebox SOHO 6tc-50 user models.

Critical Accounting Policies

Our discussion and analysis of financial condition and results of operations is based on our consolidated financial statements, which have been prepared in accordance with accounting principles generally accepted in the United States. The preparation of financial statements in conformity with generally accepted accounting principles requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. On an ongoing basis, we evaluate significant estimates used in preparing our financial statements, including those related to (i) revenue recognition, including sales returns and allowances, (ii) the provision for bad debt, (iii) inventory reserves, (iv) restructuring reserves, (v) the allocation of the purchase price in business combinations to intangible assets and (vi) analysis of impairment of goodwill and intangible assets. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, the results of which form the basis for making judgments about the carrying values of assets and liabilities that are not readily apparent from other sources. Actual results may differ from these estimates if our assumptions change or if actual circumstances differ from those in our assumptions.

We believe the following critical accounting policies affect the more significant judgments and estimates used in preparing our consolidated financial statements.

Revenue Recognition

Revenue recognition rules for software companies are very complex. Although we follow very specific and detailed guidelines in measuring revenue, certain judgments affect the application of our revenue policy. The complexity of the revenue recognition rules and estimates inherent in the revenue recognition process makes revenue results difficult to predict, and any shortfall in revenue or delay in recognizing revenues could cause our operating results to vary significantly from quarter to quarter and could result in future operating losses.

We generate revenues through:

- sales of products and service subscriptions indirectly through our distribution network at a discount from list price;
- sales of products and service subscriptions directly and, from time to time, indirectly through our distributors, to our service provider customers at volume pricing rates; and
- sales of service subscription renewals directly to end-users.

Product revenues include:

- sales of our security appliance and the perpetual software license fees for our Firebox products that are bundled with the sale of our security appliance as part of our security solutions;
- revenues from sales of software options, such as user expansion and software management modules;
- hardware sales of our RapidStream "Secured by CheckPoint" line of high performance security appliances;
- sales of our ServerLock products and anti-virus solutions for server content, application and desktop security; and
- revenues from sales of our NOC security suite software license as part of our managed security solution.

Revenues from products are generally recognized upon delivery if persuasive evidence of an arrangement exists, collection is probable, the fee is fixed and determinable, and vendor-specific objective evidence of fair

value for undelivered elements of the arrangement has been established. While we generally recognize product revenues upon shipment, revenues on product sales for some of our major distributors are recorded when these distributors have sold the product to their customers.

Service revenues primarily include the initial fees for our LiveSecurity Service subscriptions, which have periods ranging from 90 days to one year and are sold as part of our security solutions, and for LiveSecurity Service subscription renewals, which have periods ranging from one to two years, from our enterprise customers and end-users. These service fees provide our customers access to our LiveSecurity Service for product updates, security threat responses, general security information and technical support. These service fees also enable our service provider customers access to the LiveSecurity Service and the ability to manage and update a specific number of their customers' security appliances. Service subscription revenues are recognized ratably on a monthly basis, generally over periods ranging from 90 days to two years.

When service fees are bundled with the sales of our products in multiple element arrangements, the elements of those arrangements are unbundled using our objective evidence of the fair value of the undelivered elements represented by our customary pricing for each element when sold in separate transactions. Since customers receive the services over a period of time, WatchGuard determines the fair value of the service portion of the arrangement as an undelivered element, based on the renewal price of the service. Changes in the composition of such multiple-element arrangements, our ability to identify the existence of the vendor-specific objective evidence for the elements in the arrangement or our ability to estimate the fair value of elements in the arrangement could materially impact the amount of earned and unearned revenue.

We have established allowances for estimated returns, return rights and pricing protection rights. We also established an allowance for promotional rebates that may be earned by our customers. We estimate these reserves and adjust them periodically based on historical rates of returns and allowances, as well as the expected effect of current promotional programs and new product introductions. We estimate the allowance for promotional rebates based on the maximum amounts potentially available to the customers, unless we accumulate sufficient historic evidence for individual customers with respect to their realization of rebates. If new or expanded promotional programs are introduced, or new products are announced, additional allowances may be required. Alternatively, if actual promotional rebates fall below maximum exposure levels, we may reduce the allowances and recognize additional revenue.

Bad Debts

We maintain allowances for doubtful accounts for estimated losses resulting from the inability of our customers to make required payments. Significant judgment is required when we assess the ultimate realization of receivables, including the probability of collection and the creditworthiness of each customer. If the financial condition of our customers were to deteriorate, resulting in an impairment of their ability to make payments, additional allowances might be required.

Inventory Valuation

Our inventories are stated at the lower of cost or market, with cost being determined on a first-in, first-out basis. We write our inventories down to estimated market value based on assumptions about future demand and market conditions. Variation in market trends, customer preferences and introduction of new products that replace existing products or technological advances could, however, significantly affect these estimates and result in additional inventory write-downs.

Restructuring

In 2001 and 2002, we recorded significant accruals related to our restructuring plans. These accruals included estimates related to the abandonment of excess facilities. We had to adjust the restructuring accruals due to continued poor real estate market conditions in the areas where these excess facilities are located. The actual costs related to the restructuring may differ from our estimate if it takes us longer than expected to find suitable

tenants for excess facilities or if there are further changes in the real estate market in those areas where excess facilities are located. Any additional adjustments resulting from these factors could have a material effect on our financial condition and operating results.

Accounting for Goodwill and Other Intangibles

Our business acquisitions have resulted in, and future acquisitions typically will result in, the recording of goodwill, which represents the excess of the purchase price over the fair value of assets acquired as well as capitalized technology and other definite-lived intangible assets.

Effective January 1, 2002, we adopted the provisions of Statement of Financial Accounting Standards, or SFAS, No. 141, "Business Combinations," and SFAS No. 142, "Goodwill and Other Intangible Assets." SFAS No. 141 required business combinations initiated after June 30, 2001 to be accounted for using the purchase method of accounting and broadens the criteria for recording intangible assets apart from goodwill.

SFAS No. 142 requires that purchased goodwill and certain indefinite-lived intangibles no longer be amortized, but instead be tested for impairment at least annually and written down and charged to results of operations only in periods in which the recorded value of those assets exceeds their fair value.

Before 2002, we amortized goodwill on a straight-line basis over its estimated useful life of five years. With the required adoption of SFAS No. 142, beginning January 1, 2002, we no longer amortize goodwill into earnings.

SFAS No. 142 prescribes the use of the two-phase approach for testing goodwill for impairment. The first phase is a screen for potential impairment, while the second phase, if necessary, measures the amount of impairment, if any. During 2002 we completed our first phase impairment analysis and found no instances of impairment. Accordingly, the second testing phase was not required.

Separable intangible assets that do not have indefinite lives continue to be amortized over their useful lives. These assets are also periodically reviewed for potential impairment indicators.

Effective January 1, 2002, we adopted the provisions of SFAS No. 144, "Accounting for the Impairment or Disposal of Long-Lived Assets." SFAS No. 144 supercedes SFAS No. 121, "Accounting for the Impairment of Long-Lived Assets and Long-Lived Assets to be Disposed Of," and the accounting and reporting provisions relating to the disposal of a segment of a business in Accounting Principles Board Opinion No. 30. In accordance with SFAS No. 144, the carrying value of intangible assets, other than goodwill, and other long-lived assets is reviewed on a regular basis for the existence of facts or circumstances, both internal and external, that may suggest impairment.

Acquisition of RapidStream, Inc.

On April 2, 2002, we acquired RapidStream, a privately held provider of high-performance, ASIC-based firewall and VPN appliances. The acquisition of RapidStream brought advanced ASIC technology and a family of high-performance systems that allows us to address customers that require a high-performance security solution with enterprise-level networking functionality and VPN scalability. Immediately after the RapidStream acquisition, WatchGuard announced a partnership with Check Point to deliver a new class of high-performance VPN and security appliances integrating Check Point next-generation software. These "Secured by Check Point" appliances were developed by RapidStream.

The acquisition of RapidStream had a significant impact on our financial position and operating results in 2002. Specifically:

- product revenues increased during 2002 due to sales of ASIC-based products originating from our acquisition of RapidStream, which we began shipping late in the second quarter of 2002. Given the current economic uncertainty, however, it is difficult to predict revenue levels in future quarters;
- product returns may increase due to sales of future products resulting from the acquisition;

- stock-based compensation increased due to deferred stock-based compensation associated with the acquisition;
- we recorded additional amounts for goodwill and other intangible assets;
- amortization expense on definite-lived intangibles increased;
- we recorded a restructuring charge of approximately \$3.7 million in the second quarter of 2002 and an additional \$3.0 million was recorded in the fourth quarter of 2002, as we implemented a plan primarily designed to eliminate redundancies and excess headcount resulting from the acquisition. This plan included a reduction in workforce, consolidation of excess facilities and elimination of technology-related contracts that are no longer required or part of our strategy; and
- we expended approximately \$18.2 million in cash in the second quarter of 2002 for consideration paid as part of the purchase price, acquisition-related costs and additional costs of closing. This expenditure was partially offset by \$2.2 million in cash held by RapidStream at the time of the acquisition.

Results of Operations

The following table provides financial data for the periods indicated as a percentage of total revenues:

	<u>Year Ended December 31,</u>		
	<u>2000</u>	<u>2001</u>	<u>2002</u>
Revenues:			
Product	85.7 %	72.9 %	70.5 %
Service	14.3	27.1	29.5
Total revenues	100.0	100.0	100.0
Cost of revenues:			
Product	31.2	32.1	26.3
Service	4.9	9.1	7.9
Total cost of revenues	36.1	41.2	34.2
Gross margin	63.9	58.8	65.8
Operating expenses:			
Sales and marketing	39.9	46.2	44.6
Research and development	22.9	29.3	27.6
General and administrative	9.9	12.0	10.3
Stock-based compensation	13.8	14.7	1.9
Amortization of goodwill	1.7	11.4	—
Amortization and impairment of other intangible assets acquired	4.7	5.6	14.6
Acquired in-process technology	7.2	—	1.6
Restructuring charges	—	5.8	10.7
Total operating expenses	100.1	125.1	111.4
Operating loss	(36.2)	(66.3)	(45.7)
Interest income, net	10.7	9.0	3.9
Loss before income taxes	(25.5)	(57.3)	(41.8)
Provision for income taxes	0.4	0.2	—
Net loss	<u>(25.8)%</u>	<u>(57.5)%</u>	<u>(41.8)%</u>

Years Ended December 31, 2001 and 2002

Revenues

Total revenues, which consist of product revenues and service revenues, increased from \$64.3 million in 2001 to \$75.5 million in 2002, an increase of 17%. The increase in total revenues reflects a 28% increase in service revenues and a 13% increase in product revenues. The increase in service revenues resulted from

amortization of previous deferrals attributable to bundled product revenues and amortization of the renewals of LiveSecurity Service subscriptions by our existing customer base. The increase in product revenues reflects an increase in units shipped as a result of new product releases and improved sales channel performance.

We categorize our revenues into three geographic regions: the Americas, Europe/Middle East/Africa, or EMEA, and Asia Pacific, or APAC. Revenue information by geographic region, in dollars and as a percentage of total revenues, was as follows (dollars in thousands):

	Year Ended December 31,			
	2001		2002	
Americas	\$30,171	47%	\$33,363	44%
EMEA	21,414	33	27,043	36
APAC	12,698	20	15,094	20
Total	<u>\$64,283</u>	<u>100%</u>	<u>\$75,500</u>	<u>100%</u>

Revenue information for countries representing more than 10% of total revenues, in dollars and as a percentage of total revenues, was as follows (dollars in thousands):

	Year Ended December 31,			
	2001		2002	
United States	\$28,473	44%	\$31,335	42%
Japan	7,572	12	9,629	13
United Kingdom	*	*	8,753	12

* Less than 10%

Revenue information for customers representing more than 10% of total revenues, in dollars and as a percentage of total revenues, was as follows (dollars in thousands):

	Year Ended December 31,			
	2001		2002	
Tech Data	\$6,596	10%	\$10,375	14%
Ingram Micro	8,701	14	9,466	13
CDW	*	*	7,322	10

* Less than 10%

Product revenues increased from \$46.9 million in 2001 to \$53.2 million in 2002, an increase of 13%. Product revenues as a percentage of total revenues decreased from 73% in 2001 to 70% in 2002, due to a lower growth rate associated with continued slowing of economic conditions, and an increase in service revenues from an increased base of customers renewing their LiveSecurity Service subscriptions. Given the current economic uncertainty and slowdown in capital spending, it is difficult to predict product revenue levels in future quarters, which may remain depressed or fluctuate more than they have historically. We may be unable to maintain or increase the demand for our products, our revenues may not continue to grow at the same rate as in the past or at the rate expected, and we may be unable to achieve similar results in future periods.

Service revenues increased from \$17.4 million in 2001 to \$22.3 million in 2002, an increase of 28%. The increase in service revenues is due to a greater number of installed products in 2002 and to an increase in LiveSecurity Service renewals. As a percentage of total revenues, service revenues increased from 27% in 2001 to 30% in 2002, which reflects an increased base of customers renewing their LiveSecurity Service subscriptions and a reduced growth rate for product sales. We expect a slower growth rate of service revenue in 2003.

The provision for sales returns and allowances was \$6.9 million, or 10% of total revenues before returns and allowances, in 2001 and \$4.6 million, or 6% of total revenues before returns and allowances, in 2002. The higher provision in 2001 reflects the major product replacement of the Firebox II with the Firebox III undertaken in 2001, in combination with related promotional rebates associated with selling residual Firebox II inventory and the introduction of Firebox III products. The decrease in the provision in 2002 as a percentage of revenue reflects improved trends in actual returns and allowances. We expect to continue to introduce new products each year, which may affect our reserve for sales returns and allowances.

Cost of Revenues and Gross Margin

Total cost of revenues, which includes product and service costs, decreased from \$26.5 million in 2001 to \$25.9 million in 2002, a decrease of 2%. As a percentage of total revenues, cost of revenues decreased from 41% in 2001 to 34% in 2002. Correspondingly, gross margins, as a percentage of total revenues, increased from 59% in 2001 to 66% in 2002. Gross margins are affected by various factors, including the volume discount levels contained in our channel partner agreements, the cost of our Firebox and RapidStream "Secured by Check Point" appliances, expense associated with a provision for inventory reserves, lower of cost or market assessment of inventory carrying value, fixed manufacturing overhead, the mix of product and service sales, which may include hardware and software products and service subscriptions, or both, the cost of royalties associated with our products, promotional programs, and the costs of our technical support organization and LiveSecurity Service.

Cost of product revenues, which includes the cost of manufacturing our security appliances, distribution operations, product packaging and third-party product licensing fees, decreased from \$20.7 million in 2001 to \$19.9 million in 2002, a decrease of 4%. Cost of product revenues as a percentage of total revenues decreased from 32% in 2001 to 26% in 2002 and, as a percentage of product revenues, decreased from 44% in 2001 to 37% in 2002. The dollar and percentage decrease of cost of product revenues in 2002 is due to the introduction of new products with higher product margins and more favorable pricing obtained from original equipment manufacturers.

We expect an absolute dollar increase in cost of product revenues in 2003, if we achieve the expected increase in shipments. We expect product gross margins to increase in 2003, primarily as a result of increased volume combined with a more favorable product mix aimed at a greater quantity of higher-margin products. However, our gross margins may be adversely affected in the future by competitive selling pressures, the impact on the existing inventory values when replacement products are introduced and availability of key components.

Cost of service revenues, which includes the costs of our technical support organization and costs associated with our LiveSecurity Service, increased from \$5.8 million in 2001 to \$6.0 million in 2002, an increase of 2%. As a percentage of total revenues, cost of service revenues decreased from 9% in 2001 to 8% in 2002 and, as a percentage of service revenues, cost of service decreased from 34% in 2001 to 27% in 2002. The percentage decrease in cost of service revenue is primarily due to a broader customer base. We expect service costs to continue to increase in absolute dollars as our user base expands. In the longer term, as revenues from LiveSecurity Service subscriptions increase and account for a greater percentage of total revenues, we expect our service margins to increase.

Operating Expenses

Sales and Marketing. Sales and marketing expenses include salaries, commissions and employee-related expenses and certain variable marketing expenses, including distributor promotional costs, public relations costs, marketing collateral and trade show expenses. Sales and marketing expenses increased from \$29.7 million in 2001 to \$33.7 million in 2002, an increase of 13%. As a percentage of total revenues, sales and marketing expenses decreased from 46% in 2001 to 45% in 2002. The dollar increase in sales and marketing expenses was primarily due to increases in payroll and related costs from headcount increases associated with the realignment of our sales and marketing organization beginning in the fourth quarter of 2001 and from the RapidStream

acquisition, and to higher commissions expense associated with increased revenues. These increases were partially offset by a reduction in travel expenditures. Specifically, salaries, commissions, recruiting, consulting and related expenses increased from \$12.5 million in 2001 to \$16.5 million in 2002, an increase of 24%.

We expect that sales and marketing expenses will increase in 2003 in absolute dollars in connection with our continued investment in sales and marketing programs designed to increase distribution through our reseller network. We expect sales and marketing expenses to decrease as a percentage of revenue as we focus on improving depth and productivity of our existing channel partners.

Research and Development. Research and development expenses include salaries, costs of noncapitalized equipment and software tools, depreciation of capital equipment and software, costs associated with our security appliance prototypes and payments to designers and contractors. Research and development expenses increased from \$18.9 million in 2001 to \$20.9 million in 2002, an increase of 11%. As a percentage of total revenues, research and development expenses decreased from 29% in 2001 to 28% in 2002 due to the revenue increase being greater than the increase in research and development expenses. The dollar increase in research and development expenses reflects the increased employee-related expenses resulting from the RapidStream acquisition, as well as product integration costs to accelerate the rollout of new products associated with the RapidStream acquisition. Specifically, major components of the increase included:

- an increase in payroll and related expenses from \$11.6 million to \$14.6 million, the majority of which is a result of our acquisition of RapidStream; and
- an increase in security appliance prototype development and consulting costs from \$3.0 million to \$3.5 million, related to expanded product offerings in 2002 and integration of the new RapidStream and Firebox products.

We expect research and development expenses to increase in absolute dollars and decline as a percentage of revenue in 2003. We will continue to provide sufficient funding to our research and development effort in order to meet the changing requirements of our customers, to ensure continued development of new products as technology advances, and to enhance and expand our current product offerings.

General and Administrative. General and administrative expenses include costs of executive, human resource, finance and administrative support functions, provisions for uncollectible accounts and legal and accounting professional services. General and administrative expenses increased from \$7.7 million in 2001 to \$7.8 million in 2002, an increase of 1%. As a percentage of total revenues, general and administrative expenses decreased from 12% in 2001 to 10% in 2002 due to the revenue increase being greater than the increase in general and administrative expenses. The dollar increase in general and administrative expenses reflects the expansion of our infrastructure to manage the growth of our operations. The increase was partially offset by the reduction in bad debt expenses. The fluctuations in major components of total general and administrative expenses included:

- an increase in payroll and consulting and related expenses from \$3.8 million to \$4.2 million, the majority of which is related to our acquisition of RapidStream;
- an increase in business insurance from \$470,000 to \$680,000, primarily reflecting changes in market price for premiums for directors' and officers' insurance; and
- a \$930,000 decrease in bad debt expense as a result of tighter credit policies implemented during a period of changing global economic conditions and fewer small direct channel customers.

We expect general and administrative expenses to increase in absolute dollars and decline as a percentage of revenue in 2003, as we incur additional costs related to the growth of our business and our operation as a public company, including new regulatory and corporate governance requirements.

Stock-Based Compensation. Stock-based compensation expenses arise from amortization of previously deferred stock-based compensation over the vesting periods of common stock subject to repurchase and stock options. Amortization of deferred stock-based compensation expenses was \$9.4 million in 2001 and \$1.5 million in 2002. In 2001, the allocation of stock-based compensation expense was \$220,000 for sales and marketing, \$9.2 million for research and development and \$35,000 for general and administrative. In 2002, the allocation of the stock-based compensation expenses associated with the functional operating expense categories was \$62,000 for sales and marketing, \$1.3 million for research and development, and \$100,000 for general and administrative.

Deferred stock-based compensation is recorded as a component of stockholders' equity as the difference between the exercise price of options and the fair value of our common stock on the date of grant, and for the value of common stock subject to repurchase that we issued in connection with our October 1999 acquisition of BeadleNet, our October 2000 acquisition of Qiave and our April 2002 acquisition of RapidStream. In addition, deferred stock-based compensation is recorded for the fair value of stock options granted to consultants. We recorded \$558,000 of deferred stock-based compensation in 2002 in connection with the RapidStream acquisition.

Amortization of Goodwill. Amortization of goodwill related to our acquisitions of BeadleNet and Qiave was \$7.3 million in 2001. Amortization of goodwill was discontinued in 2002 due to the adoption on January 1, 2002 of SFAS No. 142, "Goodwill and Other Intangible Assets," which provides that goodwill no longer be amortized but instead be periodically reviewed for impairment. During the last quarter of 2002, we performed the required annual impairment analysis of goodwill. No impairment of goodwill was identified.

Amortization and Impairment of Other Intangible Assets Acquired. Amortization of other intangible assets acquired consists of amortization of capitalized technology and other definite-lived intangibles related to our acquisitions of Qiave and RapidStream. The intangible assets associated with our acquisition of BeadleNet in 1999 were fully amortized in 2001. We are amortizing the intangible assets on a straight-line basis over useful lives ranging from two to five years. We recorded amortization charges related to these intangible assets of \$3.6 million in 2001 and we recorded amortization and impairment of these intangible assets of \$11.1 million in 2002. The increase in amortization and impairment of other intangible assets acquired in 2002 resulted primarily from the following major factors.

- During the fourth quarter of 2002, we developed a business plan that, because of limited resources, de-emphasized further development and integration of the Qiave technology. Separately, we continued to realize lower than expected revenue from products based on Qiave technology. As a result, the expected future cash flows were determined to be insufficient to support the carrying value of the Qiave capitalized technology. We therefore recorded an impairment charge of \$6.7 million of capitalized technology related to the acquisition of Qiave.
- In 2002, we recorded \$1.5 million amortization of new intangible assets related to the acquisition of RapidStream.

We expect our amortization of other intangible assets to decrease in 2003 compared to 2002 due to the impairment charge described above.

Acquired In-Process Technology. Acquired in-process technology expenses of \$1.2 million in 2002 consists of in-process research and development, or IPR&D, expense related to our acquisition of RapidStream.

Restructuring Charges. We carried out restructuring plans in both 2001 and 2002.

In the second quarter of 2001, we announced a restructuring plan designed to streamline operations and reduce operating costs. This restructuring plan included a reduction in workforce and a consolidation of excess facilities, in addition to other cost-saving strategies. As part of the restructuring plan, we exited the consumer security market and terminated various original equipment manufacturer agreements to develop products and services for that market, and streamlined operations in support of new products and services aimed at business

customers. In 2001, we recorded a \$3.7 million restructuring charge. Additional restructuring charges of \$1.4 million were recorded in 2002, relating to revised estimates of the costs associated with the consolidation and sublease of excess facilities.

As part of this reorganization, we implemented a workforce reduction of 50 employees, which represented approximately 16% of our employee base at that time and included employees from all of our functional areas. All these employees were terminated prior to June 30, 2001. Other expenses associated with the reorganization consisted of stock-based compensation expense associated with the acceleration of vesting of stock subject to repurchase and stock options held by terminated employees, the discontinuation of the consumer security market products and the abandonment of facilities and equipment. Costs that related to ongoing operations were not included as restructuring charges. All restructuring charges have been paid as of December 31, 2002, except accrued amounts primarily related to losses for the lease buyout or sublease of abandoned facilities, which are expected to be realized through August 2010. Revenues recorded from the consumer security market were insignificant prior to the restructuring. The charges recorded to results of operations in 2001 and 2002, related to the restructuring plan of 2001, were as follows (in thousands):

	<u>Restructuring Charges in 2001</u>	<u>Restructuring Charges in 2002</u>
Severance and termination benefits	\$1,015	\$ —
Stock-based compensation	579	—
Abandoned facilities and other	<u>2,126</u>	<u>1,383</u>
Total	<u>\$3,720</u>	<u>\$1,383</u>

In the second quarter of 2002, we implemented a second restructuring plan primarily designed to eliminate redundancies and excess headcount resulting from the acquisition of RapidStream, which included a reduction in workforce, consolidation of excess facilities and elimination of technology-related contracts that are no longer required or part of our strategy. As a result of this restructuring, we recorded a \$6.7 million restructuring charge in 2002. The components of this restructuring charge for 2002 included the following (in thousands):

	<u>Restructuring Charges in 2002</u>
Severance and termination benefits	\$ 529
Costs related to cancellation of technology-related contracts	637
Abandoned facilities and other	<u>5,542</u>
Total	<u>\$6,708</u>

As part of this reorganization, we implemented a workforce reduction of 36 employees, which represented approximately 10% of our post-acquisition employee base and included employees from all of our functional areas. All of these employees were terminated prior to June 30, 2002. Other costs associated with the reorganization consist of contract terminations and the consolidation of excess facilities. Costs that related to ongoing operations were not included as restructuring charges. Restructuring charges for severance and termination benefits were paid by December 31, 2002, while accrued amounts related to losses for the lease buyout or sublease of abandoned facilities are expected to be realized through 2010. Costs of eliminating technology contracts were realized in the first quarter of 2003.

Interest Income

Interest income is generated from the investment of proceeds from the sale of common stock in our initial public offering in 1999 and our follow-on public offering in February 2000. Interest income decreased from \$5.8 million in 2001 to \$2.9 million in 2002. This decrease resulted from both a decrease in the average balance of invested funds, due primarily to cash used for the acquisition of RapidStream, as well as from a decrease in the average rates of return.

Income Taxes

Income tax expense of \$157,000 in 2001 and \$29,000 in 2002 primarily relates to our provision for foreign income taxes associated with our international operations. We have experienced losses since inception, resulting in a net operating loss carryforward position for federal income tax purposes of approximately \$185.9 million as of December 31, 2002. These carryforwards, if not utilized, will begin to expire in 2011, and may be subject to limitations under Section 382 of the Internal Revenue Code of 1986, as amended.

Years Ended December 31, 2000 and 2001

Revenues

Total revenues increased from \$60.7 million in 2000 to \$64.3 million in 2001, an increase of 6%. The increase represents an increase in service revenues, which offset a decrease in product revenues. We believe the decrease in product revenues can be attributed to slowing economic conditions that resulted in a delay or deferral in customer spending, changes in our sales and marketing organizations and a realignment of our distribution and channel customer strategy. The increase in service revenues resulted from previous deferrals attributable to bundled product revenues and the renewals of LiveSecurity Service subscriptions by our existing customer base.

Revenue information by geographic region, in dollars and as a percentage of total revenues, was as follows (dollars in thousands):

	Year Ended December 31,			
	2000		2001	
Americas	\$29,710	49%	\$30,171	47%
EMEA	19,267	32	21,414	33
APAC	11,726	19	12,698	20
Total	<u>\$60,703</u>	<u>100%</u>	<u>\$64,283</u>	<u>100%</u>

Revenue information for countries representing more than 10% of total revenues, in dollars and as a percentage of total revenues, was as follows (dollars in thousands):

	Year Ended December 31,			
	2000		2001	
United States	\$27,503	45%	\$28,473	44%
Japan	*	*	7,572	12

* Less than 10%

Revenue information for customers representing more than 10% of total revenues, in dollars and as a percentage of total revenues, was as follows (dollars in thousands):

	Year Ended December 31,			
	2000		2001	
Ingram Micro	\$7,306	12%	\$8,701	14%
Tech Data	6,366	10	6,596	10

Product revenues decreased from \$52.0 million in 2000 to \$46.9 million in 2001, a decrease of 10%. Product revenues as a percentage of total revenues decreased from 86% in 2000 to 73% in 2001, due to a lower growth rate associated with slowing economic conditions, as well as the events of September 11, 2001 and their aftermath, and an increase in service revenues from an increased base of customers renewing their LiveSecurity Service subscriptions. The decrease in product revenues was also influenced by changes in our sales and marketing organizations, and a realignment of our distribution and channel customer strategy.

Service revenues increased from \$8.7 million in 2000 to \$17.4 million in 2001, an increase of 100%. The increase in service revenues is due to a greater number of installed products in 2001 and an increase in LiveSecurity Service renewals. As a percentage of total revenues, service revenues increased from 14% in 2000 to 27% in 2001, which reflects an increased base of customers renewing their LiveSecurity Service subscriptions and a reduced growth rate for product sales.

The provision for sales returns and allowances was \$1.9 million, or 3% of total revenues before returns and allowances, in 2000 and \$6.9 million, or 10% of total revenues before returns and allowances, in 2001. The 2001 increase in the provision as a percentage of revenue reflects the major product replacement of the Firebox II with the Firebox III, promotional rebates associated with selling residual inventories of Firebox II products and the introduction of our Firebox III related products.

Cost of Revenues and Gross Margin

Total cost of revenues, which includes product and service costs, increased from \$21.9 million in 2000 to \$26.5 million in 2001, an increase of 21%. As a percentage of total revenues, cost of revenues increased from 36% in 2000 to 41% in 2001.

Cost of product revenues increased from \$18.9 million in 2000 to \$20.7 million in 2001, an increase of 9%. The dollar increase was primarily due to an \$861,000 expense increase relating to our provision for inventory reserves, a \$464,000 write-down of existing Firebox II-related inventory and higher fixed manufacturing overhead. Cost of product revenues as a percentage of total product revenues increased from 36% in 2000 to 44% in 2001. The increase in cost of product revenues as a percentage of product revenues reflects increases from the items noted above, as well as the revenue effect of promotional programs on certain existing and new Firebox products established to facilitate the introduction of several new products during 2001. The increase also reflects a change in product mix, in which the sales volume of some of our lower-margin products increased on a relative basis from 2000 to 2001.

Cost of service revenues increased from \$3.0 million in 2000 to \$5.8 million in 2001, an increase of 95%. As a percentage of total service revenues, cost of service revenues was 34% in both 2000 and 2001. Cost of service revenues as a percentage of total service revenues remained level, reflecting an increase in the investment in our customer support organization that coincides with an increasingly growing number of customers who are implementing VPNs in a more complex environment, as well as a broader customer base.

Operating Expenses

Sales and Marketing. Sales and marketing expenses increased from \$24.2 million in 2000 to \$29.7 million in 2001, an increase of 23%. As a percentage of total revenues, sales and marketing expenses increased from 40% in 2000 to 46% in 2001. The dollar increase in sales and marketing expenses was primarily due to recruiting and supporting a greater number of current and prospective resellers and distributors and to increased efforts to establish brand recognition of our products and services. Specifically, major components of the increase included:

- an increase in salaries, commissions, recruiting, consulting and related expenses from \$10.7 million to \$12.5 million; and
- an increase in variable marketing costs from \$7.8 million to \$10.6 million related to specific marketing activities designed to increase brand awareness.

Research and Development. Research and development expenses increased from \$13.9 million in 2000 to \$18.9 million in 2001, an increase of 36%. As a percentage of total revenues, research and development expenses increased from 23% in 2000 to 29% in 2001. The dollar increase in research and development expenses reflects the growth of our research and development organization to expand and enhance our Firebox System and managed security solution product lines and ServerLock products, and our efforts to respond to new and

emerging worldwide Internet security threats through our LiveSecurity Service. Specifically, major components of the increase included:

- an increase in payroll and related expenses from \$8.8 million to \$11.6 million, a portion of which is related to the research and development costs of our ServerLock products originating from our acquisition of Qiave;
- an increase in facilities expenses from \$688,000 to \$1.9 million, which reflects both a combination of the costs associated with our new corporate headquarters and the costs of facilities originating from our acquisition of Qiave; and
- an increase in designer, contractor and security appliance prototype engineering costs from \$2.6 million to \$3.0 million, related to expanded product offerings in 2001, including Firebox III and future products.

General and Administrative. General and administrative expenses increased from \$6.0 million in 2000 to \$7.7 million in 2001, an increase of 29%. As a percentage of total revenues, general and administrative expenses increased from 10% in 2000 to 12% in 2001. The dollar increase in general and administrative expenses reflects the expansion of our infrastructure to manage the growth of our operations, including an increase in payroll and related expenses and increases in other general and administrative areas, such as professional service fees and bad debt.

Stock-Based Compensation. Amortization of deferred stock-based compensation expenses was \$8.4 million in 2000 and \$9.4 million in 2001. In 2000, the allocation of the stock-based compensation expenses associated with the functional operating expense categories was \$824,000 for sales and marketing, \$7.5 million for research and development, and \$103,000 for general and administrative. In 2001, the allocation of stock-based compensation expense was \$220,000 for sales and marketing, \$9.2 million for research and development and \$35,000 for general and administrative.

We recorded \$19.3 million of deferred stock-based compensation in 2000 in connection with the Qiave acquisition, which included charges related to the issuance of common stock subject to repurchase and the assumption of unvested Qiave employee stock options outstanding at the time of the merger. In 2001, we recorded \$213,000 in deferred stock-based compensation related to options issued to consultants.

Acquired In-Process Technology. Acquired in-process technology expenses consists of IPR&D expense related to our acquisitions of BeadleNet in October 1999 and Qiave in October 2000. We recorded a one-time IPR&D charge related to the acquisition of Qiave of \$4.4 million in 2000.

Amortization of Goodwill, Purchased Technology and Other Intangible Assets Acquired. We recorded amortization charges related to goodwill, purchased technology and other intangible assets of \$3.8 million in 2000 and \$10.9 million in 2001. The increase in amortization in 2001 resulted primarily from recording amortization of intangibles associated with our acquisition of Qiave.

Restructuring Charges. As discussed above, in 2001, we carried out a restructuring plan designed to streamline our operations and reduce operating costs. As a result of this restructuring, we recorded a \$3.7 million restructuring charge in 2001.

Interest Income

Interest income decreased from \$6.5 million in 2000 to \$5.8 million in 2001. This decrease resulted from a decrease in the average rates of return.

Income Taxes

Income tax expense of \$215,000 in 2000 and \$157,000 in 2001 primarily relates to our provision for foreign income taxes associated with our international operations.

Quarterly Results of Operations

The following tables provide our unaudited results of operations, both in dollar amounts and as a percentage of total revenues, for each quarter in the eight-quarter period ended December 31, 2002. In our opinion, this unaudited information has been prepared on the same basis as our audited consolidated financial statements. This information includes all adjustments, consisting only of normal recurring adjustments, necessary for a fair presentation of the information for the quarters presented, when read in conjunction with our consolidated financial statements and the notes to our consolidated financial statements. The results of operations for any quarter are not necessarily indicative of our future results.

	Three Months Ended							
	Mar. 31, 2001	June 30, 2001	Sept. 30, 2001	Dec. 31, 2001	Mar. 31, 2002	June 30, 2002	Sept. 30, 2002	Dec. 31, 2002
	(In thousands, except per share data)							
Consolidated Statement of Operations Data:								
Revenues:								
Product	\$ 13,284	\$ 13,255	\$12,806	\$ 7,548	\$10,558	\$ 12,500	\$14,224	\$ 15,918
Service	3,818	4,253	4,462	4,857	4,954	5,348	5,851	6,147
Total revenues	<u>17,102</u>	<u>17,508</u>	<u>17,268</u>	<u>12,405</u>	<u>15,512</u>	<u>17,848</u>	<u>20,075</u>	<u>22,065</u>
Cost of revenues:								
Product	5,267	5,425	5,214	4,752	4,297	4,870	5,332	5,389
Service	1,376	1,558	1,450	1,440	1,516	1,551	1,509	1,393
Total cost of revenues	<u>6,643</u>	<u>6,983</u>	<u>6,664</u>	<u>6,192</u>	<u>5,813</u>	<u>6,421</u>	<u>6,841</u>	<u>6,782</u>
Gross margin	10,459	10,525	10,604	6,213	9,699	11,427	13,234	15,283
Operating expenses:								
Sales and marketing	8,171	7,690	7,380	6,476	7,438	8,763	8,859	8,633
Research and development ..	5,271	4,740	4,129	4,714	4,668	6,015	5,306	4,869
General and administrative ..	1,870	1,865	2,060	1,931	2,000	2,031	1,786	1,987
Stock-based compensation ..	4,520	2,546	1,468	899	613	401	288	148
Amortization of goodwill ...	1,837	1,837	1,837	1,837	—	—	—	—
Amortization and impairment of other intangible assets acquired	887	887	887	933	721	1,219	1,219	7,896
Acquired in-process technology	—	—	—	—	—	1,179	—	—
Restructuring charges	—	2,900	—	820	—	4,272	—	3,819
Total operating expenses ..	<u>22,556</u>	<u>22,465</u>	<u>17,761</u>	<u>17,610</u>	<u>15,440</u>	<u>23,880</u>	<u>17,458</u>	<u>27,352</u>
Operating loss	(12,097)	(11,940)	(7,157)	(11,397)	(5,741)	(12,453)	(4,224)	(12,069)
Interest income, net	1,701	1,622	1,292	1,156	1,120	766	636	398
Loss before income taxes	(10,396)	(10,318)	(5,865)	(10,241)	(4,621)	(11,687)	(3,588)	(11,671)
Provision for income taxes	84	84	28	(39)	13	16	—	—
Net loss	<u>\$(10,480)</u>	<u>\$(10,402)</u>	<u>\$(5,893)</u>	<u>\$(10,202)</u>	<u>\$(4,634)</u>	<u>\$(11,703)</u>	<u>\$(3,588)</u>	<u>\$(11,671)</u>
Net loss per share(1):								
Basic and diluted	<u>\$ (0.40)</u>	<u>\$ (0.39)</u>	<u>\$ (0.22)</u>	<u>\$ (0.38)</u>	<u>\$ (0.17)</u>	<u>\$ (0.36)</u>	<u>\$ (0.11)</u>	<u>\$ (0.36)</u>
Shares used in computation of net loss per share(1):								
Basic and diluted	<u>26,348</u>	<u>26,673</u>	<u>26,839</u>	<u>27,011</u>	<u>27,117</u>	<u>32,095</u>	<u>32,341</u>	<u>32,540</u>

(1) See Notes 1 and 6 of the notes to our consolidated financial statements for an explanation of the method used to calculate basic and diluted net loss per share.

	Three Months Ended							
	Mar. 31, 2001	June 30, 2001	Sept. 30, 2001	Dec. 31, 2001	Mar. 31, 2002	June 30, 2002	Sept. 30, 2002	Dec. 31, 2002
Consolidated Statement of Operations								
Data:								
Revenues:								
Product	77.7 %	75.7 %	74.2 %	60.8 %	68.1 %	70.0 %	70.9 %	72.1 %
Service	22.3	24.3	25.8	39.2	31.9	30.0	29.1	27.9
Total revenues	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0
Cost of revenues:								
Product	30.8	31.0	30.2	38.3	27.7	27.3	26.6	24.4
Service	8.0	8.9	8.4	11.6	9.8	8.7	7.5	6.3
Total cost of revenues	38.8	39.9	38.6	49.9	37.5	36.0	34.1	30.7
Gross margin	61.2	60.1	61.4	50.1	62.5	64.0	65.9	69.3
Operating expenses:								
Sales and marketing	47.8	43.9	42.7	52.2	47.9	49.1	44.1	39.1
Research and development	30.8	27.1	23.9	38.0	30.1	33.7	26.4	22.1
General and administrative	10.9	10.7	11.9	15.6	12.9	11.4	8.9	9.0
Stock-based compensation	26.5	14.5	8.5	7.2	4.0	2.2	1.4	0.7
Amortization of goodwill	10.7	10.4	10.7	14.8	—	—	—	—
Amortization and impairment of other intangible assets acquired	5.2	5.1	5.1	7.5	4.6	6.8	6.1	35.8
Acquired in-process technology	0.0	0.0	0.0	0.0	—	6.6	—	—
Restructuring charges	0.0	16.6	0.0	6.6	—	23.9	—	17.3
Total operating expenses	131.9	128.3	102.8	141.9	99.5	133.7	86.9	124.0
Operating loss	(70.7)	(68.2)	(41.4)	(91.8)	(37.0)	(69.7)	(21.0)	(54.7)
Interest income, net	9.9	9.3	7.5	9.3	7.2	4.3	3.2	1.8
Income (loss before income taxes)	(60.8)	(58.9)	(33.9)	(82.5)	(29.8)	(65.4)	(17.8)	(52.9)
Provision for income taxes	0.5	0.5	0.2	(0.3)	0.1	0.1	—	—
Net loss	(61.3)%	(59.4)%	(34.1)%	(82.2)%	(29.9)%	(65.5)%	(17.8)%	(52.9)%

During 2001 and 2002, global economic, political and other uncertainties, as well as constrained corporate information technology spending, appeared to slow the demand for our products and services. Like most companies in the technology sector, we are experiencing a downturn in the growth rate of revenues that began in the fourth quarter of 2000 and continues through the fourth quarter of 2002. We believe that both our revenues and our operating results for the eight-quarter period presented above were negatively affected by the worldwide economic conditions and an overall reduction in capital spending by businesses. Additionally, revenues and operating results for the fourth quarter of 2001 were negatively affected by changes in our sales and marketing organizations and a realignment of our distribution and channel partner strategy. While these changes of our sales and marketing organizations negatively affected our revenues and operating results in the fourth quarter of 2001, we believe they were required to compete effectively in the global Internet security market. As a result of this realignment, as well as due to the decreases in both sales returns and allowances, we achieved greater revenues sequentially for each of the four quarters of 2002. Given the current economic uncertainty and slowdown in capital spending, it is difficult to predict product revenue levels in future quarters, which may remain depressed or fluctuate more than they have historically. We may be unable to maintain or increase the demand for our products, our revenues may not continue to grow at the same rate as in the past or at the rate expected, and we may be unable to achieve similar results in future periods.

Beginning in the first quarter of 2002, sequential quarterly revenues increased by \$3.1 million, \$2.3 million, \$2.2 million and \$2.0 million, resulting in total revenues of \$15.5 million, \$17.8 million, \$20.1 million and \$22.1

million for the four sequential quarters of 2002. The revenues in the second, third and fourth quarters of 2002 were higher than the revenues in the second quarter of 2001, which was the highest revenue level achieved in 2001.

Our gross margins in 2001, both in dollars and as a percentage of total revenues, remained relatively flat until the fourth quarter of 2001, when we experienced a sharp decline in gross margins. Gross margins in the fourth quarter of 2001 were affected by the factors described above, as well as by a change in product mix that resulted in a higher concentration of lower-priced, lower-margin products being sold, fixed manufacturing overhead and customer support costs spread over a smaller revenue base, and the write-down of existing Firebox II products and related assets. During 2001, Firebox II product promotional programs that we established to facilitate the introduction of the new Firebox III product line also negatively affected gross margins. Our gross margins, both in dollars and as a percentage of total revenues, have increased sequentially in each of the four quarters of 2002 beginning with the gross margins of the fourth quarter of 2001, primarily due to higher revenues, including revenues from the initial sale of ASIC-based products, a 2002 product mix of higher margin products, and a nonrecurring write-down of Firebox II products in the fourth quarter of 2001.

Overall, our total operating expenses have fluctuated, in dollars and as a percentage of revenues, in the eight-quarter period ended December 31, 2002, due primarily to the acquisition of RapidStream in 2002 and to restructuring charges in both 2001 and 2002.

The components of the total operating expenses fluctuated as follows:

- Sales and marketing expenses increased in the first two quarters of 2002 compared to the last quarter of 2001 and were relatively flat for the third and fourth quarters of 2002. The higher sales and marketing expenses in 2002 reflect changes in our sales and marketing organizations and the realignment of our distribution and channel partner strategy, as well as increased sales commissions associated with increased revenues.
- Research and development expenses increased in the second quarter of 2002 as a result of the RapidStream acquisition, reflecting additional personnel and general development costs, and returned to the level comparable to that of 2001 by the last quarter of 2002, as a result of eliminating duplicate resources during our restructuring in the second quarter of 2002.
- General and administrative expenses have been relatively stable for the eight-quarter period ended December 31, 2002.
- Stock-based compensation charges, associated mainly with the acquisition of Qiave in October 2000, have decreased each sequential quarter since the third quarter of 2001, due primarily to recognizing a much larger portion of the expense in the early quarters after an acquisition.
- Amortization of goodwill was recorded in all quarters of 2001, but was discontinued in the first quarter of 2002 as a result of the required adoption of SFAS No. 142 on January 1, 2002.
- Amortization of other intangible assets acquired increased in the second quarter of 2002 as we capitalized technology acquired in connection with the RapidStream acquisition. In the fourth quarter of 2002, we recorded a \$6.7 million impairment charge of the capitalized technology related to the acquisition of Qiave, as we revised downwards our estimate of future cash flow streams from products based on this technology.
- IPR&D expense was recorded as a one-time cost in the second quarter of 2002 in connection with the acquisition of RapidStream.
- Restructuring charges were recorded in the second and fourth quarters of 2001 and the second and fourth quarters of 2002 associated with our 2001 and 2002 restructuring plans. In the fourth quarter of 2002, we revised upwards our estimates of restructuring losses on abandoned facilities due to the continued poor real estate market conditions in the areas where these excess facilities are located.

Liquidity and Capital Resources

As of December 31, 2002, we had \$89.3 million in cash, cash equivalents and short-term investments, which were invested primarily in high-quality money market accounts and marketable securities. We believe that the market risk arising from our holdings of these financial instruments is not material. We currently have outstanding a \$3.0 million unconditional letter of credit that we issued in September 2000 to our landlord in conjunction with the building lease for our corporate headquarters. Currently, our letter of credit is collateralized by short-term investments with our bank. Our working capital as of December 31, 2002 was \$69.5 million.

Operating Activities

Our operating activities resulted in net cash outflows of \$2.0 million in 2001 and \$7.2 million in 2002. The operating cash outflows during these periods resulted primarily from significant investments in sales and marketing and research and development, all of which led to operating losses. Net losses for 2001 and 2002 exceeded cash used in operating activities primarily as a result of non-cash charges included in net losses totaling \$23.2 million in 2001 and \$16.8 million in 2002. These non-cash charges were primarily associated with the amortization and impairment of other intangibles, amortization of goodwill in 2001, depreciation and amortization of capital assets, and compensation charges resulting from the issuance of stock options and common stock subject to repurchase by WatchGuard. Cash provided by working capital components for operating activities was \$11.8 million in 2001 and \$7.6 million in 2002. In 2002, there were large fluctuations within some of our major working capital components, as described below:

- (a) *Net Receivables* increased from \$6.4 million at December 31, 2001 to \$8.8 million at December 31, 2002, primarily reflecting the increase in revenues from \$12.4 million for the three months ended December 31, 2001 to \$22.1 million for the three months ended December 31, 2002. Days sales outstanding, or DSOs, calculated on a quarterly basis, improved from 46 days at December 31, 2001 to 36 days at December 31, 2002. DSOs are affected by the payment terms contained in our customer contracts, risks associated with the uncertain economy, whether revenues in a particular quarter are linear (that is, are evenly distributed throughout the quarter or weighted more toward the end of the quarter), and the amount of deferred revenue contained in the receivable balance that has not been recognized as revenue. Based on our current sales mix, the linearity of revenues in past and future quarters, timing differences arising from the varying payment terms in our customer agreements and the growth of deferred revenue, we expect our DSOs to generally range from 50 to 60 days in the future. Any change in these factors, however, could negatively affect expected DSO results.
- (b) *Accounts Payable and Accrued Expenses* increased from \$7.5 million at December 31, 2001 to \$10.0 million at December 31, 2002. The increase resulted from corresponding increases in sales and marketing, research and development and general and administrative expenses in the last quarter of 2002 compared to the last quarter of 2001. Those expenses increased from \$13.1 million in the fourth quarter of 2001 to \$15.5 million in the fourth quarter of 2002.
- (c) *Accrued Restructuring and Acquisition Costs* increased from \$1.5 million at December 31, 2001 to \$9.0 million at December 31, 2002. The increase is related primarily to the remaining \$1.6 million of acquisition liabilities assumed in connection with the acquisition of RapidStream, and to the remaining amounts of the restructuring liabilities of \$550,000 for the 2001 restructuring plan and \$5.4 million for the 2002 restructuring plan as of December 31, 2002.
- (d) *Deferred Revenue* increased from \$15.7 million at December 31, 2001 to \$18.5 million at December 31, 2002. This increase reflects the deferral of revenue from bundled LiveSecurity Service subscriptions included in new product revenues and renewals of LiveSecurity Service subscriptions from a growing customer base.

Investing Activities

Cash provided by investing activities was \$121,000 in 2001 and \$352,000 in 2002. During 2001, these activities primarily related to short-term investment of the proceeds received from our public offerings, offset by capital expenditures for equipment and furniture. During 2002, these activities primarily related to short-term investment of the proceeds received from our public offerings, offset by the net cash consideration paid in connection with the acquisition of RapidStream. To complete the acquisition of RapidStream, we expended approximately \$17.3 million in cash in 2002, net of acquired RapidStream cash balances, including consideration paid as part of the purchase price, settlement of acquisition-related costs and additional costs of closing.

Financing Activities

Cash provided by financing activities totaled \$2.0 million in 2001 and \$1.8 million in 2002. Cash provided by financing activities in both periods reflects the exercise of employee stock options and the purchase of common stock through our employee stock purchase plan.

We believe that our existing cash and securities balances will be sufficient to meet our anticipated cash needs for the increased operating expenses associated with the acquisition of RapidStream, for other potential acquisitions or technology investments, for our announced plan to potentially repurchase up to \$8 million of our common stock and for our working capital and capital expenditures for at least the next 12 months. We may need to seek additional funding before that time through public or private financings or other arrangements, however, if the underlying assumed levels of spending for other potential acquisitions or investments in complementary businesses or technologies prove to be inaccurate.

Contractual Obligations

We lease office space and some computer equipment under noncancelable operating leases. Our facilities commitments include a lease for our corporate headquarters in Seattle, Washington, which expires in September 2010. We have the option to extend this lease for an additional five-year term. We also lease a product fulfillment and distribution warehouse in Seattle, with a lease term through April 2006. We lease facilities in Aliso Viejo and San Jose, California and Waltham, Massachusetts under operating leases that expire in years between 2004 and 2006, in addition to leases for other sales offices under operating leases or other lease obligations that expire over various terms. Our excess facilities at our corporate headquarters in Seattle, and in Aliso Viejo and San Jose, California, are partially subleased to tenants, with sublease terms that expire between 2003 and 2007. We also have several operating leases for computer equipment. WatchGuard is also a party to several noncancelable and nonrefundable agreements to purchase inventory.

Our contractual commitments at December 31, 2002 associated with lease obligations, purchase obligations and other long-term liabilities, net of future minimum rental income from subleases of \$1.1 million, are as follows (in thousands):

<u>Contractual Obligations</u>	<u>Payment due by period</u>				
	<u>Total</u>	<u>Less than 1 year</u>	<u>1-3 years</u>	<u>3-5 years</u>	<u>More than 5 years</u>
Operating lease obligations	\$24,497	\$4,142	\$6,781	\$6,034	\$7,540
Purchase obligations	2,831	2,831	—	—	—
Total	<u>\$27,328</u>	<u>\$6,973</u>	<u>\$6,781</u>	<u>\$6,034</u>	<u>\$7,540</u>

Other Commitments

In the event that the average of the high and low sales prices of WatchGuard common stock on April 2, 2003, the first anniversary of the closing date of the acquisition of RapidStream, is less than the average of the

high and low sales prices of WatchGuard common stock on April 2, 2002, the closing date of the merger, WatchGuard will make an aggregate cash payment to the former holders of RapidStream common stock equal to the product of 0.42 multiplied by the difference between (i) the average trading price on the closing date, \$6.32, discounted to reflect the effect on fair market value of the lockup restrictions on the shares of WatchGuard common stock issued to the former RapidStream shareholders and (ii) the average trading price on the first anniversary of the closing date, multiplied by the number of shares of WatchGuard common stock issued to and held by the former holders of RapidStream common stock, or up to approximately 915,000 shares. WatchGuard expects that any payment, if required, would not be material to its financial position. This payment, if required, will be a downward adjustment to the additional paid-in capital, reflecting the reduction in value of securities issued in the transaction.

ITEM 7A. QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

Interest Rate Risk. We do not hold derivative financial instruments or derivative equity securities in our investment portfolio. Our cash equivalents and short-term investments consist of high-quality securities, as specified in our investment policy guidelines. Our policy limits the amount of credit exposure to any one issue or issuer to a maximum of 20% of the total portfolio or \$5 million per issuer at the time of purchase, with the exception of U.S. treasury and agency securities and money market funds, which are exempt from this size limitation. Our policy limits all investments to those that mature in two years or less, with the average maturity of our investments equal to one year or less. The securities are subject to interest-rate risk and will decrease in value if interest rates increase. The fair value of our investment portfolio or related income would not be significantly affected by either a 100 basis point increase or decrease in interest rates, due primarily to the short-term nature of the major portion of our investment portfolio, which is summarized in Note 4 to our notes to consolidated financial statements.

Foreign Currency Risk. All of our sales and the majority of our expenses are currently denominated in U.S. dollars. As a result, we have not experienced significant foreign exchange gains and losses. While we incurred some expenses in foreign currencies during 2001 and 2002 and expect to continue to do so in the future, we do not anticipate that foreign exchange gains or losses will be material to us. Although we have not engaged in foreign currency hedging to date, we may do so in the future.

ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA

REPORT OF ERNST & YOUNG LLP, INDEPENDENT AUDITORS

Board of Directors and Stockholders
WatchGuard Technologies, Inc.

We have audited the accompanying consolidated balance sheets of WatchGuard Technologies, Inc. as of December 31, 2001 and 2002 and the related consolidated statements of operations, stockholders' equity, and cash flows for each of the three years in the period ended December 31, 2002. Our audits also included the financial statement schedule listed in the Index at Item 15(a). These financial statements and schedule are the responsibility of WatchGuard's management. Our responsibility is to express an opinion on these financial statements and schedule based on our audits.

We conducted our audits in accordance with auditing standards generally accepted in the United States. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the financial statements referred to above present fairly, in all material respects, the consolidated financial position of WatchGuard Technologies, Inc. at December 31, 2001 and 2002, and the consolidated results of its operations and its cash flows for each of the three years in the period ended December 31, 2002, in conformity with accounting principles generally accepted in the United States. Also, in our opinion, the related financial statement schedule, when considered in relation to the basic financial statements taken as a whole, presents fairly in all material respects the information set forth therein.

As discussed in Note 2 to the consolidated financial statements, the Company changed its method of accounting for goodwill and other intangible assets as a result of adopting the provisions of the Statements of Financial Accounting Standards No. 142, "Goodwill and Other Intangible Assets," effective January 1, 2002.

ERNST & YOUNG LLP

Seattle, Washington
February 3, 2003

WATCHGUARD TECHNOLOGIES, INC.
CONSOLIDATED BALANCE SHEETS
(In thousands, except share and per share data)

	December 31,	
	2001	2002
ASSETS		
Current assets:		
Cash and cash equivalents	\$ 13,958	\$ 8,890
Short-term investments	99,785	80,412
Trade accounts receivable, net	6,363	8,813
Inventories, net	4,413	4,442
Prepaid expenses and other	4,000	4,435
Total current assets	128,519	106,992
Property and equipment, net	7,383	6,467
Goodwill, net	26,991	66,605
Other intangibles, net and other assets	10,138	9,234
Total assets	\$173,031	\$ 189,298
LIABILITIES AND STOCKHOLDERS' EQUITY		
Current liabilities:		
Accounts payable	\$ 4,032	\$ 4,905
Accrued expenses and other liabilities	3,500	5,143
Accrued restructuring and acquisition costs	1,486	9,035
Deferred revenues	15,709	18,451
Total current liabilities	24,727	37,534
Commitments and contingencies		
Stockholders' equity:		
Preferred stock, \$0.001 par value:		
Authorized shares: 10,000,000		
No shares issued and outstanding	—	—
Common stock, \$0.001 par value:		
Authorized shares: 80,000,000		
Shares issued and outstanding: 27,123,260 at December 31, 2001 and 32,655,404 at December 31, 2002	27	33
Additional paid-in capital	231,533	265,932
Deferred stock-based compensation	(1,357)	(254)
Accumulated other comprehensive income	681	229
Accumulated deficit	(82,580)	(114,176)
Total stockholders' equity	148,304	151,764
Total liabilities and stockholders' equity	\$173,031	\$ 189,298

See accompanying notes.

WATCHGUARD TECHNOLOGIES, INC.
CONSOLIDATED STATEMENTS OF OPERATIONS
(In thousands, except per share data)

	Year Ended December 31,		
	2000	2001	2002
Revenues:			
Product	\$ 52,010	\$ 46,893	\$ 53,200
Service	8,693	17,390	22,300
Total revenues	60,703	64,283	75,500
Cost of revenues:			
Product	18,932	20,658	19,888
Service	2,987	5,824	5,969
Total cost of revenues	21,919	26,482	25,857
Gross margin	38,784	37,801	49,643
Operating expenses:			
Sales and marketing (1)	24,213	29,717	33,693
Research and development (2)	13,900	18,854	20,858
General and administrative (3)	6,001	7,726	7,804
Stock-based compensation	8,407	9,433	1,450
Amortization of goodwill	1,005	7,347	—
Amortization and impairment of other intangible assets acquired	2,823	3,595	11,055
Acquired in-process technology	4,399	—	1,179
Restructuring charges	—	3,720	8,091
Total operating expenses	60,748	80,392	84,130
Operating loss	(21,964)	(42,591)	(34,487)
Interest income, net	6,515	5,771	2,920
Loss before income taxes	(15,449)	(36,820)	(31,567)
Provision for income taxes	215	157	29
Net loss	<u>\$(15,664)</u>	<u>\$(36,977)</u>	<u>\$(31,596)</u>
Basic and diluted net loss per share (4)	<u>\$ (0.66)</u>	<u>\$ (1.38)</u>	<u>\$ (1.02)</u>
Shares used in calculation of basic and diluted net loss per share	<u>23,556</u>	<u>26,723</u>	<u>31,029</u>

(1) Sales and marketing expenses exclude amortization of stock-based compensation of \$824,000, \$220,000 and \$62,000 for 2000, 2001 and 2002, respectively.

(2) Research and development expenses exclude amortization of stock-based compensation of \$7,480,000, \$9,178,000 and \$1,288,000 for 2000, 2001 and 2002, respectively.

(3) General and administrative expenses exclude amortization of stock-based compensation of \$103,000, \$35,000 and \$100,000 for 2000, 2001 and 2002, respectively.

(4) See Notes 1 and 6 of the notes to our consolidated financial statements for an explanation of the method used to calculate basic and diluted net loss per share.

See accompanying notes.

WATCHGUARD TECHNOLOGIES, INC.
CONSOLIDATED STATEMENTS OF STOCKHOLDERS' EQUITY
(In thousands, except share data)

	Common Stock Shares	Common Stock Amount	Additional Paid-In Capital	Deferred Stock-Based Compensation	Accumulated Other Comprehensive Loss	Accumulated Deficit	Total Stockholders' Equity
Balance, January 1, 2000	19,511,752	\$ 19	\$ 63,694	\$ (1,452)	\$ (77)	\$ (29,939)	\$ 32,245
Proceeds from issuance of common stock from public offering, net of offering costs	1,780,000	2	90,425	—	—	—	90,427
Deferred stock-based compensation	—	—	19,342	(19,342)	—	—	8,407
Amortization of stock-based compensation	—	—	—	8,407	—	—	—
Issuance of common stock in connection with the BeadleNet acquisition	20,189	—	—	—	—	—	50,303
Issuance of common stock in connection with the QIave acquisition	1,292,997	1	50,302	—	—	—	5,693
Exercise of common stock options and warrants	3,597,202	3	5,690	—	—	—	1,139
Issuance of common stock in conjunction with the employee stock purchase program	84,932	1	1,138	—	—	—	(145)
Comprehensive loss:	—	—	—	—	(145)	—	(15,664)
Net unrealized loss on securities available for sale	—	—	—	—	—	—	(15,809)
Net loss	—	—	—	—	—	—	172,405
Comprehensive loss	—	—	—	—	(222)	(45,603)	161
Balance, December 31, 2000	26,287,072	26	230,591	(12,387)	—	—	9,851
Deferred stock-based compensation	—	—	213	(213)	—	—	—
Stock compensation related to acceleration of option vesting	—	—	161	9,851	—	—	—
Amortization of stock-based compensation	—	—	—	—	—	—	—
Adjustment of deferred stock-based compensation for options cancelled upon employee terminations	—	—	(1,392)	1,392	—	—	895
Exercise of common stock options and warrants	722,566	1	894	—	—	—	1,066
Issuance of common stock in conjunction with the employee stock purchase program	113,622	—	1,066	—	—	—	903
Comprehensive loss:	—	—	—	—	903	—	(36,977)
Net unrealized gain on securities available for sale	—	—	—	—	—	—	(36,074)
Net loss	—	—	—	—	—	—	148,304
Comprehensive loss	—	—	—	—	681	(82,580)	1,450
Balance, December 31, 2001	27,123,260	27	231,533	(1,357)	—	—	—
Amortization of stock-based compensation	—	—	—	1,450	—	—	—
Adjustment of deferred stock-based compensation for options cancelled upon employee terminations	—	—	(211)	211	—	—	—
Issuance of common stock and stock options in connection with acquisition of RapidStream	4,915,690	5	32,810	(558)	—	—	32,257
Repurchase of unvested restricted common stock upon employee terminations	(3,964)	(6)	(6)	—	—	—	(6)
Exercise of common stock options	452,717	1	1,057	—	—	—	1,058
Issuance of common stock in conjunction with the employee stock purchase program	167,701	—	749	—	—	—	749
Comprehensive loss:	—	—	—	—	(452)	—	(452)
Net unrealized loss on securities available for sale	—	—	—	—	—	—	(31,596)
Net loss	—	—	—	—	—	—	(32,048)
Comprehensive loss	—	—	—	—	—	—	\$151,764
Balance, December 31, 2002	32,655,404	\$ 33	\$265,932	\$ (254)	\$ 229	\$ (114,176)	\$151,764

See accompanying notes.

WATCHGUARD TECHNOLOGIES, INC.
CONSOLIDATED STATEMENTS OF CASH FLOWS
(In thousands)

	Year Ended December 31,		
	2000	2001	2002
Operating activities:			
Net loss	\$ (15,664)	\$ (36,977)	\$ (31,596)
Adjustments to reconcile net loss to net cash used in operating activities:			
Depreciation and amortization of property and equipment	1,400	2,236	2,827
Amortization of goodwill	1,005	7,347	—
Amortization and impairment of other intangible assets acquired	2,823	3,595	11,055
Amortization of stock-based compensation	8,407	10,012	1,450
Acquired in-process technology	4,399	—	1,179
Other	—	—	291
Changes in operating assets and liabilities:			
(Increase) decrease in accounts receivable	(11,496)	8,908	(2,240)
(Increase) decrease in inventories	(5,013)	2,613	598
(Increase) in prepaid expenses and other	(1,903)	(822)	(248)
(Increase) in other assets	(43)	(75)	(17)
Increase (decrease) in accounts payable and accrued expenses	6,034	(4,119)	897
Increase in restructuring and acquisition costs	—	1,486	5,921
Increase in deferred revenue	7,641	3,835	2,663
Net cash used in operating activities	(2,410)	(1,961)	(7,220)
Investing activities:			
Purchases of equipment, furniture and other	(6,369)	(2,275)	(1,251)
Proceeds from sales of marketable securities	—	61,907	51,034
Proceeds from maturities of marketable securities	85,474	124,112	88,924
Purchases of marketable securities	(162,399)	(183,623)	(121,038)
Net cash (paid) acquired in connection with acquisitions	762	—	(17,317)
Net cash (used in) provided by investing activities	(82,532)	121	352
Financing activities:			
Principal repayments on line of credit, long-term debt and notes payable ..	(383)	—	—
Proceeds from sale of common stock, net of expenses	90,427	—	—
Proceeds from the exercise of common stock options and warrants and the sale of common stock through the employee stock purchase plan	6,832	1,961	1,800
Net cash provided by financing activities	96,876	1,961	1,800
Net increase in cash and cash equivalents	11,934	121	(5,068)
Cash and cash equivalents at beginning of period	1,903	13,837	13,958
Cash and cash equivalents at end of period	<u>\$ 13,837</u>	<u>\$ 13,958</u>	<u>\$ 8,890</u>
Supplemental disclosure of cash flow information:			
Cash paid for interest	<u>\$ 51</u>	<u>\$ —</u>	<u>\$ —</u>
Reversal of deferred stock-based compensation for options cancelled upon employee termination	<u>\$ —</u>	<u>\$ 1,392</u>	<u>\$ 211</u>

See accompanying notes.

WATCHGUARD TECHNOLOGIES, INC.
NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

1. Accounting Policies

Description of Business

WatchGuard Technologies, Inc. (WatchGuard) is a leading global provider of Internet security solutions designed to protect enterprises that use the Internet for electronic commerce and secure communications.

Revenue Recognition

WatchGuard recognizes revenue in accordance with accounting standards for software companies, including Statement of Position (SOP) 97-2, "Software Revenue Recognition," as amended by SOP 98-9, and related interpretations, including Technical Practice Aids. In December 1999, the Securities and Exchange Commission (SEC) issued Staff Accounting Bulletin (SAB) 101, "Revenue Recognition in Financial Statements." SAB 101 summarizes certain of the SEC's views in applying generally accepted accounting principles to revenue recognition in financial statements. WatchGuard believes its current revenue recognition policies and practices are consistent with the current accounting standards.

WatchGuard generates revenues through sales of its Firebox and RapidStream "Secured by Check Point" products, including related software licenses, subscriptions for its LiveSecurity Service, which includes access to technical support, software updates (if and when available), threat responses, expert editorials, support flashes, virus alerts and interactive training, and sales of ServerLock products. Software license revenues are generated from licensing the rights to use WatchGuard's products directly to end-users, from sublicense fees from resellers and distributors and from sales of its managed security solution products to Internet service providers and other service providers that utilize WatchGuard's products to provide managed security services to their customers.

Revenues from software license agreements are generally recognized upon delivery of software if persuasive evidence of an arrangement exists, collection is probable, the fee is fixed and determinable, and vendor-specific objective evidence of fair value for undelivered elements of the arrangement has been established. Vendor-specific objective evidence is typically based on the price charged when an element is sold separately or, if an element is not sold separately, on the price established by authorized management, if it is probable that the price, once established, will not change before market introduction. WatchGuard uses the residual method, as defined in SOP 98-9, to allocate revenues to delivered elements once it has established vendor-specific objective evidence for all undelivered elements. Under the residual method, any discount in the arrangement is allocated to the delivered element.

WatchGuard provides allowances for estimated returns and return rights and pricing protection rights, which are offered to most customers. WatchGuard also provides allowances for promotional rebates offered to its customers. A customer's return rights are generally limited to the lesser of its on-hand inventory or a percentage of the customer's purchases for the previous quarter. Pricing protection rights, offered to many of WatchGuard's customers, are generally limited to 60 to 90 days after notification of a price change. Revenues are reduced by the provision for estimated returns and allowances at the time the sales are made.

The promotional rebates vary by type and term and are earned by customers in accordance with various conditions. WatchGuard accounts for promotional rebates given to customers in accordance with the Emerging Issues Task Force (EITF) Issue No. 01-09, "Accounting for Consideration Given by a Vendor to a Customer or a Reseller of the Vendor's Product," which requires that sales incentives given to customers or resellers be accounted for as a reduction of revenue unless a vendor receives a benefit that is identifiable and can be reasonably estimated. WatchGuard accrues the maximum amount possible unless historical trends indicate a lower rate of accrual is adequate.

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

Some of WatchGuard's distributors have unlimited stock return and rotation rights. Revenues from these distribution arrangements are not recognized until the distributors sell the products to their customers. Revenues from LiveSecurity Service subscriptions are recognized ratably over the term of the contract, typically 90 days to two years. WatchGuard's payment terms typically range from 30 to 60 days.

Principles of Consolidation

The consolidated financial statements include the accounts of WatchGuard and its wholly owned subsidiaries. All significant intercompany accounts and transactions are eliminated in consolidation.

Fair Values of Financial Instruments

At December 31, 2002, WatchGuard had the following financial instruments: cash and cash equivalents, short-term investments, accounts receivable, accounts payable and accrued expenses. The carrying value of cash and cash equivalents, accounts receivable, accounts payable and accrued expenses approximate their fair value based on the liquidity of these financial instruments or their short-term nature.

Cash Equivalents

WatchGuard considers all highly liquid investments purchased with maturities of three months or less at the date of purchase to be cash equivalents. Cash equivalents are carried at fair market value. Cash equivalents consist of money market funds.

Short-Term Investments

WatchGuard's investments, consisting entirely of commercial paper and corporate and government debt securities, are classified as available for sale, and are stated at fair value with unrealized gains and losses included as a component of stockholders' equity. The amortized cost of investments is adjusted for amortization of premiums and accretion of discounts to maturity. The amortizations and accretions are included in interest income. Realized gains and losses, declines in value of securities judged to be other than temporary, and interest and all dividends earned on securities are also included in interest income. The cost of securities sold is calculated using the specific identification method. WatchGuard's investment guidelines state that the maximum life of any one security shall be two years, with the maximum weighted average life of the investment portfolio being one year.

Inventories

Inventories are stated at the lower of cost or market, with cost being determined on a first-in, first-out basis. WatchGuard's inventory costs include the freight and handling costs incurred to transport goods from WatchGuard's suppliers. WatchGuard receives some of its components from single-source suppliers and relies on a limited number of hardware manufacturers. Inventories located at distributors who have unlimited return rights are included in finished goods. In assessing the ultimate realization of inventories, WatchGuard is required to make judgements as to future demand requirements and compare these with the current or committed inventory levels. WatchGuard writes down its inventory for estimated obsolescence or unmarketable inventory. The reserve requirements fluctuate due to market conditions, customer preferences and technological and product life-cycle changes.

Property and Equipment

Property and equipment is stated at cost, less accumulated depreciation and amortization. Equipment and furniture is depreciated using the straight-line method over estimated useful lives ranging from three to five years. Leasehold improvements are amortized over the shorter of the lease term or the estimated useful life.

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

Goodwill

Beginning on January 1, 2002, with the adoption of Statement of Financial Accounting Standards (SFAS) No. 142, "Goodwill and Other Intangible Assets," goodwill and other indefinite lived intangibles are no longer amortized, but instead tested for impairment on an annual basis or on an interim basis if indications of impairment are present. Prior to 2002, goodwill related to acquisitions was amortized on a straight-line basis over the period of expected benefit of three to five years.

Intangible Assets with Definite Lives and Other Long-Lived Assets

Intangible assets with definite lives, including primarily current technology received in connection with acquisitions, are amortized over their estimated useful lives ranging from three to five years. In accordance with SFAS No. 144, "Accounting for the Impairment or Disposal of Long-Lived Assets," the carrying value of intangible assets with definite lives and other long-lived assets is reviewed on a regular basis for the existence of facts that may indicate that the assets are impaired. Such asset is considered impaired when its estimated future cash flows are less than the amount of its carrying value. If the carrying value of this asset is deemed not recoverable, it is adjusted downwards to the asset's estimated fair value. In 2002, WatchGuard identified and recorded the impairment of the developed technology acquired from Qiave in 2000 (see Note 2).

Research and Development

Research and development costs, which consist primarily of software development costs, are expensed as incurred. SFAS No. 86, "Accounting for the Costs of Computer Software to Be Sold, Leased, or Otherwise Marketed," requires the capitalization of certain software development costs after technological feasibility of the software is established. In the development of WatchGuard's new products and enhancements to existing products, the technological feasibility of the software is not established until substantially all product development is complete, including the development of a working model. Internal software development costs that were eligible for capitalization were insignificant and were charged to research and development expense in WatchGuard's consolidated statements of operations.

Internal-Use Software

WatchGuard recognizes costs of software developed or purchased for internal-use in accordance with SOP 98-1, "Accounting for Costs of Computer Software Developed or Obtained for Internal Use." Under SOP 98-1, WatchGuard expenses all costs incurred that relate to planning and post-implementation phases of development. Costs incurred in the development and implementation phases are capitalized and amortized over the estimated useful life of software. In 2002, WatchGuard capitalized the development costs of \$169,000 for internal-use software. Because costs incurred during the development stage were insignificant, no costs related to internal-use software were capitalized in 2001 and 2000.

Advertising Costs

WatchGuard expenses advertising costs as incurred. Total advertising expenses were \$711,000, \$885,000 and \$1.2 million in 2000, 2001 and 2002, respectively.

Concentration of Credit Risk

WatchGuard is subject to concentrations of credit risk primarily from cash investments and accounts receivable. WatchGuard manages its credit risk by investing its excess cash in a diverse portfolio of high quality

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

money market instruments and short-term investments. In addition, substantially all of WatchGuard's accounts receivable are due from WatchGuard's resellers, distributors and service providers located throughout the world. Sales to customers outside the United States were \$33.2 million, \$35.8 million and \$44.2 million, or 55%, 56% and 58% of total revenues, for 2000, 2001 and 2002, respectively. No foreign country accounted for more than 10% of revenues in 2000. Sales to Japan accounted for 12% of total revenues during 2001. Sales to Japan and the United Kingdom in 2002 accounted for 13% and 12%, respectively, of revenues in 2002. During 2000 and 2001, two customers accounted for 22% and 24%, respectively, of total revenues. During 2002, three customers accounted for 37% of total revenues. Geographic regions accounting for 10% or more of revenues were the Americas with 49%, 47% and 44% of total revenues, Europe/Middle East/ Africa (EMEA) with 32%, 33% and 36% of total revenues, and Asia Pacific (APAC) with 19%, 20% and 20% of total revenues, for 2000, 2001 and 2002, respectively. WatchGuard does not require collateral or other security to support credit sales, but provides an allowance for bad debts based on historical experience and specifically identified risks.

Stock-Based Compensation

WatchGuard has elected to apply the disclosure-only provisions of SFAS No. 123, "Accounting for Stock-Based Compensation." Accordingly, WatchGuard accounts for stock-based compensation using the intrinsic value method prescribed in Accounting Principle Board (APB) Opinion No. 25, "Accounting for Stock Issued to Employees," and related interpretations. Compensation cost for stock options is measured as the excess, if any, of the fair value of WatchGuard's common stock at the date of grant over the stock option exercise price. Pro forma information required by SFAS No. 123 is included in Note 5.

Stock compensation expense for options or warrants granted to non-employees has been determined in accordance with EITF Issue No. 96-18, "Accounting for Equity Instruments That Are Issued to Other Than Employees for Acquiring, or in Conjunction with Selling, Goods or Services" and is based on the fair value of the equity instruments issued. The fair value of options granted to non-employees is periodically measured as the underlying options vest.

Income Taxes

WatchGuard recognizes deferred tax assets and liabilities based on differences between the financial reporting and tax bases of assets and liabilities using the enacted tax rates and laws that are expected to be in effect when the differences are expected to be recovered. WatchGuard provides a valuation allowance for deferred tax assets that cannot be currently recognized due to WatchGuard's cumulative losses and the uncertainty of future recoverability.

Comprehensive Income (Loss)

WatchGuard complies with SFAS No. 130, "Reporting Comprehensive Income," which establishes standards for reporting and displaying comprehensive income and its components (revenues, expenses, gains and losses) in a full set of general-purpose financial statements. WatchGuard's comprehensive loss includes net loss and the effect of unrealized gains or losses on securities available for sale. Comprehensive loss is shown on the consolidated statement of stockholders' equity.

Net Loss Per Share

Basic and diluted net loss per share is calculated using the average number of shares of common stock outstanding. Other common stock equivalents, including stock options, are excluded from the computation because their effect is antidilutive.

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

Use of Estimates

The preparation of financial statements in conformity with generally accepted accounting principles requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. Actual results could differ from those estimates. Significant estimates used in preparing the attached financial statements relate to (i) revenue recognition, including sales returns and allowances, (ii) provision for bad debt, (iii) inventory reserves, (iv) restructuring reserves relating to abandoned facilities, (v) the allocation of the purchase price in business combinations to intangible assets and (vi) fair values and impairment analysis of goodwill and intangible assets with definite lives.

Segment Information

SFAS No. 131, "Disclosures About Segments of an Enterprise and Related Information," establishes standards for reporting information about operating segments in annual financial statements. It also establishes standards for related disclosures about products, services, geographical areas and major customers. WatchGuard operates in a single business segment related to Internet and computer security and provides hardware, software and services as a complete security solution. See Note 10 for revenue reported by geographic area.

Reclassifications

Certain prior-year items have been reclassified to conform to the current-year presentation.

Recent Accounting Pronouncements

In July 2002, the Financial Accounting Standards Board (FASB) issued SFAS No. 146, "Accounting for Costs Associated with Exit or Disposal Activities." SFAS No. 146 addresses financial accounting and reporting for costs associated with exit or disposal activities and nullifies EITF Issue No. 94-3, "Liability Recognition for Certain Employee Termination Benefits and Other Costs to Exit an Activity (including Certain Costs Incurred in a Restructuring)." SFAS No. 146 generally requires that a liability for a cost associated with an exit or disposal activity be recognized when the liability is incurred rather than at the date of an entity's commitment to an exit plan. WatchGuard will adopt this pronouncement on January 1, 2003. As the provisions of SFAS No. 146 are effective for exit and disposal activities initiated after December 31, 2002, the adoption of this statement will not affect the operating results or financial position for periods presented.

In November 2002, the FASB issued Interpretation No. 45 (FIN 45), "Guarantor's Accounting and Disclosure Requirements for Guarantees, Including Indirect Guarantees of Indebtedness of Others." FIN 45 elaborates on the existing disclosure requirements for most guarantees such as standby letters of credits, and provides new disclosure requirements regarding indemnification provisions, including indemnification provisions typically included in a software license arrangement. It also clarifies that at the time a guarantee is issued, WatchGuard must recognize an initial liability for the fair value of the obligations it assumes under the guarantee and must disclose that information in its financial statements. The provisions related to recognizing a liability at inception of the guarantee do not apply to product warranties, indemnification provisions in WatchGuard's software license arrangements, or to guarantees accounted for as derivatives. The initial recognition and measurement provisions apply on a prospective basis to guarantees issued or modified after December 31, 2002 and the disclosure requirements apply to guarantees outstanding as of December 31, 2002. WatchGuard does not expect the adoption of FIN 45 to have material effect on its consolidated financial position and results of operations. The adoption of the disclosure requirements of this standard as of December 31, 2002 had no impact on WatchGuard's financial position or results of operations.

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

At the November 21, 2002 meeting, the Emerging Issues Task Force of the FASB reached a consensus on EITF Issue 00-21 "Revenue Arrangements with Multiple Deliverables", which addresses revenue recognition for arrangements that may involve the delivery or performance of multiple products, services, and/or rights to use assets. The final consensus will be applicable to agreements entered into in fiscal periods beginning after June 15, 2003, with early adoption permitted. To the extent that an arrangement is within the scope of other existing higher-level authoritative literature that provides guidance regarding whether and/or how to separate multiple-deliverable arrangements into separate units of accounting, including, but not limited to, Statement 13, Statement 45, Statement 66, SOP 81-1, SOP 97-2 and SOP 00-2, the arrangement should be accounted for in accordance with that literature. As WatchGuard accounts for the multiple-elements revenue arrangements in accordance with SOP 97-2, it does not believe the adoption of EITF 00-21 will have a material impact on its financial position or results of operation.

In December 2002, the FASB issued SFAS No. 148, "Accounting for Stock-Based Compensation — Transition and Disclosure." SFAS No. 148 amends SFAS No. 123, "Stock-Based Compensation," to provide alternative methods of transition for a voluntary change to the fair value based method of accounting for stock-based employee compensation. In addition, SFAS No. 148 amends the disclosure requirements of SFAS No. 123 to require prominent disclosures in both annual and interim financial statements about the method of accounting for stock-based employee compensation and the effect of the method used on reported results. The adoption of this statement did not have a material impact on WatchGuard's financial position or results of operations, as WatchGuard has not elected to change to the fair value-based method of accounting for stock-based employee compensation. The disclosure provisions of SFAS No. 148 are effective for fiscal years ended December 15, 2002 and have been incorporated into these financial statements and accompanying footnotes.

2. Accounting for Goodwill and Intangibles with Definite Lives.

In July 2001, the FASB issued SFAS No. 141, "Business Combinations," and SFAS No. 142, "Goodwill and Other Intangible Assets." SFAS No. 141 requires business combinations completed after June 30, 2001 to be accounted for using the purchase method of accounting, and broadens the criteria for recording intangible assets separate from goodwill.

SFAS No. 142 requires that goodwill and other indefinite lived intangibles no longer be amortized to earnings, but instead be tested for impairment at least annually and written down and charged to results of operations only in periods in which the recorded value of those assets exceeds their fair value. Current technology and other separable intangible assets that do not have indefinite lives are continued to be amortized over their useful lives. SFAS No. 142 prescribes the use of the two-phase approach for testing goodwill for impairment. The first phase is a screen for potential impairment, while the second phase (if necessary) measures the amount of impairment, if any.

WatchGuard adopted SFAS No. 141 and SFAS No. 142 on January 1, 2002. The transitional impairment test prescribed by SFAS No. 142 was completed as of January 1, 2002. WatchGuard completed its annual impairment test for goodwill using an October 1, 2002 measurement date. No impairment of goodwill was indicated at either date; accordingly, the second testing phase was not necessary during 2002.

Application of the new standards resulted in a reclassification to goodwill of the unamortized balance of assembled workforce intangible assets recorded with the acquisitions of BeadleNet in 1999 and Qiave in 2000 in the amount of \$390,000 on January 1, 2002. This resulted in a net goodwill balance of \$27.0 million as of January 1, 2002 (which, as of January 1, 2002, is no longer subject to amortization but will be subject to evaluation for impairment) and a net balance of other intangibles of \$9.8 million (which will continue to be

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

amortized over their estimated useful lives of three to five years). The following table summarizes the effect SFAS 142 would have had on net loss and basic and diluted net loss per share, had the statement been applied retroactively for all years presented (in thousands, except per share data):

	Year Ended December 31,		
	2000	2001	2002
Net loss			
Net loss—as reported	\$(15,664)	\$(36,977)	\$(31,596)
Adjustment for amortization of goodwill	1,005	7,347	—
Net loss—as adjusted	\$(14,659)	\$(29,630)	\$(31,596)
Basic and diluted net loss per share			
Basic and diluted net loss per share—as reported	\$ (0.66)	\$ (1.38)	\$ (1.02)
Amortization of goodwill, per share	0.04	0.27	—
Basic and diluted net loss per share—as adjusted	\$ (0.62)	\$ (1.11)	\$ (1.02)

In August 2001, the FASB issued SFAS No. 144, "Accounting for the Impairment or Disposal of Long-Lived Assets," which is effective January 1, 2002. SFAS No. 144 supercedes SFAS No. 121, "Accounting for the Impairment of Long-Lived Assets to be Disposed Of," and the accounting and reporting provisions relating to the disposal of a segment of a business in APB Opinion No. 30. In accordance with SFAS No. 144, the carrying value of intangible assets and other long-lived assets is reviewed on a regular basis for the existence of facts or circumstances, both internal and external, that may suggest impairment. During the fourth quarter of 2002, WatchGuard developed a business plan that, because of limited resources, de-emphasized further development and integration of the technology acquired from Qiave in 2000. Separately, WatchGuard continued to realize lower than expected revenue from products based on Qiave technology. In accordance with SFAS No. 144, the discounted expected future cash flows were determined to be insufficient to support the carrying value of the Qiave capitalized technology. WatchGuard therefore recorded an impairment charge of \$6.7 million of capitalized technology related to the acquisition of Qiave. The corresponding increase in accumulated amortization leaves a net balance of \$186,000.

The following table summarizes other intangibles, net and other assets as of December 31, 2001 and December 31, 2002 (in thousands):

	December 31, 2001	December 31, 2002
Current technology	\$13,376	\$ 23,342
Accumulated amortization	(3,614)	(14,675)
	9,762	8,667
Other assets	376	567
	\$10,138	\$ 9,234

Current technology will be amortized over their remaining useful lives through 2007. The remaining amortization is expected to be \$2.1 million, \$2.1 million, \$2.0 million, \$2.0 million and \$500,000 for the years 2003, 2004, 2005, 2006 and 2007, respectively.

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

3. Balance Sheet Account Detail

Trade Accounts Receivable, Net

Trade accounts receivable, net consisted of the following (in thousands):

	December 31,	
	2001	2002
Trade accounts receivable	\$ 9,202	\$11,144
Reserve for returns and allowances	(2,046)	(1,845)
Allowance for uncollectible accounts	(793)	(486)
	\$ 6,363	\$ 8,813

Inventories, Net

Inventories, net consisted of the following (in thousands):

	December 31,	
	2001	2002
Finished goods	\$4,015	\$3,811
Components	746	1,256
	4,761	5,067
Inventory reserves	(348)	(625)
	\$4,413	\$4,442

Property and Equipment, Net

Property and equipment, net consisted of the following (in thousands):

	December 31,	
	2001	2002
Computer equipment	\$ 4,403	\$ 4,944
Leasehold improvements	2,587	2,299
Furniture and equipment	2,721	3,362
Software	1,894	2,787
	11,605	13,392
Less accumulated depreciation and amortization	(4,222)	(6,925)
	\$ 7,383	\$ 6,467

Accrued Expenses and Other Liabilities

Accrued expenses consisted of the following (in thousands):

	December 31,	
	2001	2002
Accrued payroll related liabilities	1,395	2,226
Other accrued liabilities	2,105	2,917
	\$3,500	\$5,143

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

4. Short-Term Investments

Short-term investments consisted of the following (in thousands):

	<u>Market Value</u>	<u>Gross Unrealized Gains</u>	<u>Gross Unrealized Losses</u>	<u>Amortized Cost</u>
Balance at December 31, 2001:				
Commercial paper	\$ 3,000	\$—	\$—	\$ 3,000
Corporate debt securities	47,772	442	(22)	47,352
U.S. government and agency obligations	49,013	293	(32)	48,752
	<u>\$99,785</u>	<u>\$735</u>	<u>\$ (54)</u>	<u>\$99,104</u>
Balance at December 31, 2002:				
Commercial paper	\$ 3,000	\$—	\$—	\$ 3,000
Corporate debt securities	18,798	91	(4)	18,710
U.S. government and agency obligations	58,614	146	(4)	58,473
	<u>\$80,412</u>	<u>\$237</u>	<u>\$ (8)</u>	<u>\$80,183</u>

The contractual maturities of WatchGuard's available-for-sale securities as of December 31, 2002 are as follows (in thousands):

	<u>Market Value</u>	<u>Amortized Cost</u>
Due in one year or less	\$48,892	\$48,785
Due in one year through two years	31,520	31,398
	<u>\$80,412</u>	<u>\$80,183</u>

At December 31, 2002, short-term investments were restricted by a \$3.0 million unconditional letter of credit issued to WatchGuard's landlord in conjunction with a facilities lease.

5. Stockholders' Equity

Public Offerings

On February 15, 2000, WatchGuard issued 1,780,000 shares of its common stock in a public offering, at a price of \$54.125 per share. The offering also included an additional 2,314,000 shares of common stock sold by selling stockholders, including those sold pursuant to the exercise of the underwriters' over-allotment option. The proceeds to WatchGuard from the offering were approximately \$90.4 million, net of \$5.9 million in offering expenses, underwriting discounts and commissions.

Stock Options

WatchGuard's 1996 Stock Incentive Compensation Plan (the 1996 Plan) provides for the grant of incentive and nonqualified stock options to employees, officers, directors, agents, consultants and independent contractors. At December 31, 2002, WatchGuard had reserved 10,358,766 shares of common stock for grant under the 1996 Plan. The number of shares reserved for issuance of stock options under the 1996 Plan is automatically increased on the first day of each fiscal year to the least of (a) 750,000 shares, (b) 3% of the average number of common shares outstanding used to calculate fully diluted earnings per share as reported in WatchGuard's annual financial statements for the preceding year and (c) an amount determined by the board of directors. In July 2000,

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

WatchGuard adopted the 2000 Stock Option Plan (the 2000 Plan), which provides for the granting of nonqualified stock options to employees, agents, consultants, advisors and independent contractors. As of December 31, 2002, WatchGuard had reserved 8,000,000 shares of common stock for grant under the 2000 Plan.

Options under both the 1996 Plan and the 2000 Plan generally are granted at fair market value on the date of grant. The shares of common stock covered by options granted on the date of hire generally vest at the rate of 25% on the first anniversary of the date of grant, and an additional 2.08% every month thereafter, with all shares becoming fully vested on the fourth anniversary date of the date of grant. Options granted other than on the date of hire generally vest at the rate of 2.08% every month, commencing one month from the date of grant. Stock options granted under both the 1996 Plan and the 2000 Plan have a term of ten years.

In October 2000, WatchGuard acquired Qiave Technologies Corporation. Under the terms and conditions of the acquisition, the Qiave Technologies Corporation 2000 Stock Option Plan (the Qiave Plan) was assumed by WatchGuard and all options to purchase shares of Qiave common stock outstanding at the effective time of the acquisition converted into options to purchase an aggregate of 100,856 shares of WatchGuard common stock (see Note 11) granted under the Qiave Plan.

In April 2002, WatchGuard acquired RapidStream, Inc. Under the terms and conditions of the acquisition, the RapidStream, Inc. 1998 Stock Option Plan (the RapidStream Plan) was assumed by WatchGuard and all options to purchase shares of RapidStream common stock at the effective time of the acquisition converted into options to purchase an aggregate of 318,251 shares of WatchGuard common stock (see Note 11) granted under the RapidStream Plan. At the time of acquisition, WatchGuard had reserved 645,896 shares of common stock for grant under the RapidStream Plan. The following table summarizes WatchGuard's stock option activity for all of its stock option plans during 2000, 2001 and 2002:

	2000		2001		2002	
	Options	Weighted Average Exercise Price	Options	Weighted Average Exercise Price	Options	Weighted Average Exercise Price
Balance at beginning of period	6,502,680	\$ 4.60	5,992,419	\$29.27	4,999,942	\$12.75
Granted	3,506,656	46.24	4,367,750	11.82	5,185,182	5.57
Exercised	(3,375,551)	1.69	(722,566)	1.23	(452,717)	2.34
Canceled	(641,366)	17.15	(4,637,661)	35.01	(1,978,156)	10.72
Balance at end of period	<u>5,992,419</u>	29.27	<u>4,999,942</u>	12.75	<u>7,754,251</u>	9.08
Exercisable at end of period	1,071,510		1,339,509		2,828,529	
Shares of common stock available for grant					5,193,355	

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

The weighted average remaining contractual life and weighted average exercise price of options outstanding and options exercisable at December 31, 2002 under all of WatchGuard's stock option plans for selected exercise price ranges is as follows:

Exercise Prices	Shares	Options Outstanding		Options Exercisable	
		Weighted Average Remaining Contractual Life (in years)	Weighted Average Exercise Price	Shares	Weighted Average Exercise Price
\$ 0.03 – 4.80	1,089,759	8.67	\$ 3.69	331,058	\$ 1.80
\$ 4.90 – 5.68	769,045	9.30	5.32	118,769	5.39
\$ 5.68 – 6.02	1,124,500	9.27	6.02	—	0.00
\$ 6.13 – 6.13	1,115,700	9.09	6.13	653,720	6.13
\$ 6.21 – 9.90	1,379,281	8.56	8.75	460,515	8.75
\$ 9.99 – 13.00	972,812	7.75	11.55	528,763	12.19
\$13.63 – 14.47	969,627	7.67	14.14	538,185	14.16
\$14.50 – 53.06	333,527	7.68	34.92	197,519	35.71
	<u>7,754,251</u>	8.58	\$ 9.08	<u>2,828,529</u>	\$10.74

Deferred Stock-Based Compensation

WatchGuard uses the intrinsic value-based method to account for all of its employee stock-based compensation arrangements. Therefore, compensation costs are not recognized in WatchGuard's consolidated financial statements, unless the underlying fair value of WatchGuard's common stock exceeds the exercise price of the stock options at the date of grant.

In 2000, WatchGuard recorded \$19.3 million in deferred stock-based compensation in connection with the acquisition of Qiave (see Note 11), \$4.3 million of which related to WatchGuard's assumption of unvested options to purchase Qiave common stock and \$15.0 million of which related to the issuance of WatchGuard common stock to key Qiave employees, subject to a repurchase restriction, gradually released over a 2-year period.

In 2001, WatchGuard recorded \$213,000 of deferred stock-based compensation related to 20,000 option shares granted to one consultant and 12,000 option shares granted to other consultants. Final measurement of the fair value of the 20,000 option shares occurred in 2002 and final measurement of the 12,000 options shares will occur when the options fully vest in 2005. Also, in 2001, WatchGuard recognized stock compensation of \$161,000 when it accelerated vesting provisions of an employee's stock option on his termination of employment in connection with the April 2001 restructuring.

In 2002, WatchGuard recorded \$558,000 of deferred stock-based compensation in connection with the acquisition of RapidStream (see Note 11), \$419,000 of which related to WatchGuard's assumption of unvested options to purchase RapidStream common stock and \$139,000 of which related to the issuance of WatchGuard common stock to twelve RapidStream employees, subject to a repurchase restriction, released over a 28-month period beginning on the purchase date. In 2002, WatchGuard recorded \$24,000 of deferred stock-based compensation related to 6,000 option shares granted to consultants in 2002. In addition, WatchGuard decreased by \$25,000 deferred stock-based compensation previously recorded for 2001 stock option grants to consultants, due to the remeasurement of the originally estimated fair value of these grants. Final measurement of the fair value of options granted to consultants in 2002 will not occur until the options are fully vested in 2006.

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

In 2001 and in 2002, WatchGuard also recorded \$1.4 million and \$211,000 adjustments to reduce previously recorded deferred stock-based compensation for the unvested portion of options upon termination of employees prior to vesting.

Amounts recorded as deferred stock-based compensation related to stock options are generally being amortized over the vesting period of the options (generally three to four years), using the graded vesting approach. Amortization of deferred stock-based compensation related to shares subject to repurchase is generally recognized over the term of the related employment agreements.

Stock based compensation expense was \$8.4 million, \$9.4 million and \$1.5 million in 2000, 2001 and 2002, respectively. The stock-based compensation expense in 2001 excluded \$418,000 of deferred stock compensation amortization, which was charged to restructuring, for the acceleration of options and restricted share vesting for employees terminated in connection with restructuring. In 2001 and 2002, stock-based compensation expense included \$166,000 and \$10,000 for amortization of deferred stock option expense on options issued to consultants.

Stock Option Exchange Program

On August 1, 2001, WatchGuard cancelled options to purchase 2,106,347 shares of WatchGuard common stock with exercise prices ranging from \$14.47 to \$100.19 per share. In exchange for these options, in February 2002, WatchGuard granted options to purchase 1,833,303 shares of WatchGuard common stock with exercise prices equal to \$6.1255 per share, the then fair market value of the underlying common stock. Each replacement option vested and was exercisable substantially to the same degree as the original option.

Common Stock Warrants

During 2000, certain warrants were exercised for the purchase of 15,000 shares of common stock at exercise prices ranging from \$0.03 per share to \$0.13 per share. In 2000, a warrant holder exercised a warrant to purchase 200,000 shares of common stock at an exercise price of \$0.39 per share on a net exercise basis, resulting in the issuance of 198,446 shares of common stock.

At December 31, 2002, WatchGuard had no warrants outstanding.

1999 Employee Stock Purchase Plan

The 1999 Employee Stock Purchase Plan (the ESPP) permits eligible employees of WatchGuard to purchase common stock through payroll deductions of up to 15% of their compensation. The price of the common stock purchased under the ESPP will be the lesser of 85% of the fair market value on the first day of an offering period and 85% of the fair market value on the last day of an offering period. WatchGuard authorized the issuance under the ESPP of a total of 600,000 shares of common stock, plus an automatic annual increase to be added on the first day of each fiscal year equal to the least of (a) 400,000 shares, (b) 1.5% of the average number of common shares outstanding used to calculate fully diluted earnings per share as reported in WatchGuard's annual financial statements for the preceding year and (c) an amount determined by the board of directors.

A total of 113,622 and 167,701 shares of common stock were purchased by WatchGuard employees under the ESPP during 2001 and 2002, respectively. At December 31, 2002, WatchGuard had a total of 1,120,636 shares of common stock reserved for future issuance under the ESPP.

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

Pro Forma Disclosures Under SFAS 123

The following pro forma information regarding stock-based compensation has been determined as if WatchGuard had accounted for its employee stock options and ESPP shares under the fair market value method of SFAS 123. The fair value of the employee stock options was estimated at the date of grant, using a minimum value option pricing model through the date of WatchGuard's initial public offering in July 1999 and using the Black-Scholes pricing model thereafter.

The fair value of each option granted was estimated at the date of grant, with the following weighted average assumptions as follows:

	For the Years Ended December 31,		
	2000	2001	2002
Average risk-free interest rates	6%	4%	3%
Volatility	1.36	1.14	1.05
Expected life (in years)	4 to 5	4 to 5	4 to 5
Dividend rate	0%	0%	0%

The weighted average fair values of stock options granted during 2000, 2001 and 2002 were as follows:

	For the Years Ended December 31,					
	2000		2001		2002	
	Options Granted	Average Fair Value	Options Granted	Average Fair Value	Options Granted	Average Fair Value
Exercise price equal to market price of stock on grant date	3,405,800	\$42.32	4,367,750	\$9.19	4,866,931	\$4.01
Exercise price less than market price of stock on grant date	100,856	49.54	—	—	318,251	5.80

For purposes of pro forma disclosures, the estimated fair value of the options is amortized over their vesting periods.

Pro forma disclosures are not representative of future results. During preparation of footnotes to the consolidated financial statements for fiscal 2002, WatchGuard determined that the calculation of the net loss—pro forma reported under SFAS No. 123 for 2001, as reported in that year, did not reflect the application of the fair value based method under SFAS No. 123 to WatchGuard's stock option exchange program. Accordingly, the amount of the net loss—pro forma reported under SFAS No. 123 for 2001 presented in the table below has been revised, resulting in an increase from \$49.5 million, the previously reported amount. This revision had no effect on our previously reported consolidated results of operations or financial condition.

WatchGuard's pro forma information is as follows (in thousands, except per share data):

	Year Ended December 31,		
	2000	2001 (Revised)	2002
Net loss—as reported	\$(15,664)	\$(36,977)	\$(31,596)
Add: stock-based compensation, as reported	8,407	9,433	1,450
Deduct: stock-based compensation determined under fair value based method	(47,863)	(56,374)	(32,763)
Net loss—pro forma	(55,120)	(83,918)	(62,909)
Net loss per share—as reported	(0.66)	(1.38)	(1.02)
Net loss per share—pro forma	(2.34)	(3.14)	(2.03)

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

Common Shares Reserved

At December 31, 2002, common stock reserved for future issuance was as follows:

Outstanding stock options	7,754,251
Stock options available for future grant	5,193,355
ESPP	<u>1,120,636</u>
	<u>14,068,242</u>

Stock Repurchase

On October 24, 2002, WatchGuard announced that its Board of Directors approved the repurchase by WatchGuard of up to \$8 million of its common stock. Depending on market conditions and other factors, repurchases may be made from time to time in the open market and in negotiated transactions, including block transactions, and may be discontinued at any time. As of December 31, 2002, no stock repurchases had been made.

6. Net Loss per Share

Basic and diluted net loss per common share is calculated by dividing net loss by the weighted average number of common shares outstanding. Options to purchase 5,992,419 shares, 4,999,942 shares and 7,754,251 shares of common stock at December 31, 2000, 2001 and 2002, respectively, and 250,079 shares, 74,186 shares and 8,821 shares of common stock subject to repurchase at December 31, 2000, 2001 and 2002, respectively, were excluded from the computation of basic and diluted net loss per common share, as their effect is antidilutive.

7. Income Taxes

At December 31, 2002, WatchGuard had a net operating loss carryforward for federal tax purposes of approximately \$185.9 million and research and development tax credit carryforwards of \$2.8 million. These carryforwards begin to expire after the 2011 tax year. Utilization of net operating loss carryforwards may be subject to certain limitations under Section 382 of the Internal Revenue Code. Additionally, approximately \$103.5 million of the net operating losses generated for federal income tax purposes are not available to reduce income tax expense for financial reporting purposes because the tax effects of tax deductions for employee stock options in excess of the related financial reporting compensation expense are recognized through equity. A valuation allowance has been established to reflect the uncertainty of generating future taxable income necessary to utilize available tax loss carryforwards.

WatchGuard provides for deferred taxes based on the difference between the basis of assets and liabilities for financial reporting purposes and the basis for income tax purposes, calculated using enacted rates that will be in effect when the differences are expected to reverse. Significant components of WatchGuard's deferred tax assets and liabilities are as follows (in thousands):

	December 31,	
	2001	2002
Deferred tax assets:		
Net operating loss carryforwards	\$ 51,138	\$ 64,673
Acquisition intangibles	1,818	(1,298)
Research and development tax credit	1,822	2,807
Sales reserve and allowance for bad debts	1,102	1,207
Accrued expenses and other	641	860
Restructuring charge	—	2,598
Total deferred tax assets	56,521	70,847
Valuation allowance	<u>(56,521)</u>	<u>(70,847)</u>
Net deferred taxes	<u>\$ —</u>	<u>\$ —</u>

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

WatchGuard's valuation allowance increased by \$36.7 million in 2000, \$9.6 million in 2001 and \$14.3 million in 2002.

The reconciliation of the income tax provision (benefit) calculated using the federal statutory rates to the recorded income tax provision are as follows (dollars in thousands):

	December 31,					
	2000 Tax Effected		2001 Tax Effected		2002 Tax Effected	
	Amount	Rate	Amount	Rate	Amount	Rate
Net loss before taxes	\$(15,449)		\$(36,820)		\$(31,567)	
Expected tax benefit at federal statutory rate	\$ (5,253)	34.0 %	\$(12,519)	34.0 %	\$(10,733)	34.0 %
Research and development credit	(602)	3.9	(602)	1.7	(350)	1.1
Permanent differences, including non-deductible acquisition costs	5,160	(33.4)	5,990	(16.9)	3,366	(10.7)
Tax benefit not recognized due to valuation allowance	695	(4.5)	7,131	(18.8)	7,717	(24.4)
Alternative minimum tax	36	(0.2)	—	—	—	—
Foreign tax expense	179	(1.2)	157	(0.4)	29	(0.09)
Total tax expense	<u>\$ 215</u>	<u>(1.4)%</u>	<u>\$ 157</u>	<u>(0.4)%</u>	<u>\$ 29</u>	<u>(0.09)%</u>

8. 401(k) Retirement Plan

WatchGuard sponsors a 401(k) plan that is available to all employees who satisfy certain eligibility requirements relating to minimum age, length of service and hours worked. Eligible employees may elect to contribute up to 15% of their pre-tax gross earnings, subject to statutory limitations regarding maximum contributions. WatchGuard may also make a discretionary contribution to the plan. No such contributions have been made by WatchGuard.

9. Commitments

WatchGuard leases office space and some computer equipment under noncancelable operating leases. Facilities commitments include a 10-year lease for its corporate headquarters in Seattle, Washington, which expires in September 2010. WatchGuard has the option to extend this lease for an additional five-year term. WatchGuard also leases a product fulfillment and distribution warehouse in Seattle, with the lease term through April 2006. The Company also leases facilities in Aliso Viejo and San Jose, California and Waltham, Massachusetts under operating leases that expire in years between 2004 and 2006, in addition to month-to-month leases for other sales offices under operating leases or other lease obligations that expire over various terms. Our excess facilities at our corporate headquarters in Seattle, and in Aliso Viejo and San Jose, California are partially subleased to tenants, with sublease terms that expire between 2003 and 2007. Future minimum payments at December 31, 2002 under leases for office space and computer equipment, net of future minimum rental income from sublease of \$1.1 million, are as follows (in thousands):

	Abandoned Facilities			
	Abandoned in Restructuring, net	Assumed in RapidStream Acquisition, net	Facilities and Equipment in Use	Total
2003	\$1,214	\$ 658	\$ 2,270	\$ 4,142
2004	1,029	673	2,108	3,810
2005	1,075		1,896	2,971
2006	1,079		1,877	2,956
2007	1,258		1,820	3,078
Thereafter	2,527		5,013	7,540
	<u>\$8,182</u>	<u>\$1,331</u>	<u>\$14,984</u>	<u>\$24,497</u>

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

Rent expense for 2000, 2001 and 2002 was \$1.5 million, \$2.8 million and \$3.2 million, respectively.

In addition to the foregoing lease commitments, WatchGuard is a party to several noncancelable and non-refundable agreements to purchase inventory in 2002. The total of these commitments was \$2.8 million at December 31, 2002.

10. Geographical Revenues

WatchGuard licenses and markets its Internet security products and services throughout the world, and operates in a single industry segment. While certain expenses for sales and marketing activities are incurred in various geographical regions, substantially all of WatchGuard's assets are located, and the majority of its operating expenses are incurred, at its corporate headquarters. WatchGuard categorizes revenues into three geographic regions, as shown in the table below. Revenue information by geographic region is as follows (dollars in thousands):

	Year Ended December 31,					
	2000		2001		2002	
Americas	\$29,710	49%	\$30,171	47%	\$33,363	44%
EMEA	19,267	32	21,414	33	27,043	36
APAC	11,726	19	12,698	20	15,094	20
Total	<u>\$60,703</u>	<u>100%</u>	<u>\$64,283</u>	<u>100%</u>	<u>\$75,500</u>	<u>100%</u>

Revenue information for countries representing more than 10% of total revenues is as follows (dollars in thousands):

	Year Ended December 31,					
	2000		2001		2002	
United States	\$27,503	45%	\$28,473	44%	\$31,335	42%
Japan	*		7,572	12	9,629	13
United Kingdom	*		*		8,753	12

* Less than 10%

11. Acquisitions

RapidStream, Inc.

On April 2, 2002, WatchGuard acquired all of the outstanding capital stock of RapidStream, Inc., a privately held provider of ASIC (application specific integrated circuit)-based firewall and virtual private networking (VPN) appliances. The acquisition of RapidStream brings ASIC technology that allows WatchGuard to address customers that require enterprise-level networking functionality and VPN scalability. The results of RapidStream's operations have been included in WatchGuard's consolidated financial statements since the date of acquisition.

The total RapidStream consideration of \$51.0 million was comprised of (a) \$16.5 million in cash, (b) 4.92 million shares of WatchGuard common stock valued at \$31.0 million, (c) WatchGuard's assumption of RapidStream's obligations under its stock option plan, resulting in the conversion of RapidStream options into options to purchase 318,251 shares of WatchGuard common stock valued at approximately \$1.8 million using the

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

Black-Scholes pricing model and the following assumptions: risk-free interest rate of 4.75%, an expected life of 5 years and a volatility of 1.37, and (d) \$1.7 million in professional fees related to the acquisition. Deferred stock-based compensation associated with the conversion of unvested RapidStream stock options and the issuance of restricted stock was \$558,000. An aggregate of approximately 1.2 million shares of the WatchGuard common stock issuable as merger consideration will be held in escrow for one year from the effective time of the merger, to secure the indemnification obligations of the RapidStream shareholders under the merger agreement.

In connection with the execution of the merger agreement, the officers and directors of RapidStream who were shareholders and their respective affiliates entered into a shareholders agreement. Under the terms of the shareholders agreement, these shareholders and affiliates agreed, among other things, to certain lockup restrictions on the resale of the shares of WatchGuard common stock they received in the merger. Shareholders and affiliates who owned an aggregate of 2,988,769 shares of WatchGuard common stock each agreed not to sell or otherwise transfer more than 6.25% of the WatchGuard shares received in the merger (Lockup Shares) until 90 days after the effective time of the merger, and no more than 10% of such Lockup Shares in any month thereafter until the one-year anniversary of the effective time. In addition, two shareholders who owned an aggregate of 348,233 shares of WatchGuard common stock agreed not to sell or otherwise transfer any of their Lockup Shares until two years after the effective time, except that 5% of the Lockup Shares were released from the lockup restriction three months after the effective time, 5% were released six months after the effective time, 10% will be released one year after the effective time and 20% will be released on the last day of each three-month period thereafter. Finally, one shareholder who beneficially owned 340,878 shares of WatchGuard common stock agreed not to sell or otherwise transfer any of his Lockup Shares until 90 days after the effective time and no more than 10% of his Lockup Shares in any month thereafter until the one-year anniversary of the effective time.

In the event that the average of the high and low sales prices of WatchGuard common stock on the first anniversary of the closing date, April 2, 2003, is less than the average of the high and low sales prices of WatchGuard common stock on the closing date of the merger, WatchGuard will make an aggregate cash payment to the former holders of RapidStream common stock equal to the product of 0.42 multiplied by the difference between (i) the average trading price on the closing date, \$6.32, discounted to reflect the effect on fair market value of the lockup restrictions on the Lockup Shares and (ii) the average trading price on the first anniversary of the closing date, multiplied by the number of shares of WatchGuard common stock issued to and held by the former holders of RapidStream common stock, or up to approximately 915,000 shares. This payment, if required, will be a downward adjustment to the additional paid-in capital, reflecting the reduction in value of securities issued in the transaction.

The following table summarizes the purchase price allocation as of December 31, 2002 (in thousands):

Tangible assets and liabilities	
Cash	\$ 2,183
Accounts receivable, net	210
Inventory, net	627
Property and equipment, net	944
Other assets	361
Accounts payable and accrued liabilities	(4,542)
Deferred revenue	(79)
Total fair value of RapidStream tangible assets, net of liabilities	(296)
Current technology	9,966
Goodwill	39,614
Acquired in-process research and development	1,179
Total purchase price	50,463
Deferred stock-based compensation	558
Total consideration, including deferred stock-based compensation	<u>\$51,021</u>

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

Tangible assets and liabilities. Tangible assets and liabilities are recorded at fair value. The accounts payable and accrued liabilities of approximately \$4.5 million included acquisition-related liabilities of approximately \$2.9 million for severance and termination costs associated with RapidStream employees, costs related to the abandonment of excess facilities, a liability reflecting the fair value of an over-market lease, and other costs. Amounts recorded related to these items and accrued balances remaining at December 31, 2002 were as follows (in thousands):

	Acquisition Liabilities at April 2, 2002	Amounts Paid or Charged	Balance at December 31, 2002
Severance and termination costs	\$ 606	\$ (604)	\$ 2
Over-market lease and abandoned facilities	<u>2,288</u>	<u>(711)</u>	<u>1,577</u>
Total acquisition-related liabilities	<u>\$2,894</u>	<u>\$(1,315)</u>	<u>\$1,579</u>

As part of the acquisition, WatchGuard terminated 21 employees from the original RapidStream workforce. All of these employees were terminated prior to December 31, 2002. Accrued amounts related to over-market leases and abandoned facilities are expected to be realized through 2004.

Current technology. Values assigned to current technology were determined using the income approach. Under the income approach, fair value reflects the present value of the projected cash flows that are expected to be generated by the products incorporating the current technology. To determine the value of current technology, WatchGuard discounted the expected future cash flows of the existing technology products at a rate of 15%, taking into account the weighted average cost of capital and risks related to the characteristics and applications of each product, existing and future markets and assessments of the life-cycle stage of each project. Based on this analysis, WatchGuard capitalized the existing technology that had reached technological feasibility. The projected revenues used in the income approach are based on the future revenues that will most likely be generated by the commercial sales of the technology. The current technology will be amortized over the estimated useful lives of 5 years.

Gross profit was assumed to be 58% in the partial year of 2002, 60% in 2003 and 70% in each of the remaining three years of the five-year projection period. Operating expenses, including sales and marketing, research and development and general and administrative costs, were assumed to be 79% of revenues in the initial year of the projection, declining to 29% in 2003 and 38% for each of the three remaining years.

Goodwill. The value assigned to goodwill represents the excess of the purchase price over the sum of the amounts assigned to identifiable assets acquired less liabilities assumed. A value of approximately \$39.6 million was assigned to goodwill in the acquisition. In accordance with SFAS 142, goodwill is not amortized but reviewed for impairment. The goodwill is not deductible for tax purposes.

Acquired in-process research and development. Values assigned to the acquired in-process research and development (IPR&D) were determined using an income approach. To determine the value of the IPR&D, WatchGuard considered, among other factors, the state of development of each project, the time and cost needed to complete each project, expected income and associated risks, which included the inherent difficulties and uncertainties in completing the project and achieving technological feasibility and risks related to the viability of and potential changes in future target markets. This analysis resulted in amounts assigned to IPR&D for projects that had not yet reached technological feasibility and do not have alternative future uses. The entire \$1.2 million allocated to acquired IPR&D was expensed on the date of acquisition.

At the time of the acquisition, three IPR&D projects were identified as being related to future products for which technological or commercial feasibility had not yet been established and that did not have an alternative

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

future use. WatchGuard analyzed each project, using estimated percentage completion factors ranging from less than 10% to 65%. Revenue growth rates for RapidStream's IPR&D were assumed to be as high as 175% in the year after the year of introduction and decreasing each year to a negative growth rate of 35% in the final year of the five-year projection period. Projected annual revenues related to IPR&D ranged from approximately \$1.6 million to \$5.0 million over the term of the projections. These projections were based on aggregate revenue growth rates for the business as a whole, anticipated growth rates for the Internet security market, anticipated product development and product introduction cycles and the estimated life of the underlying technology.

Gross profit was assumed to be 58% in the partial year of 2002, 60% in 2003 and 70% in each of the remaining three years of the five-year projection period. Operating expenses, including sales and marketing, research and development and general and administrative costs, were assumed to be 161% of revenues in the initial year of the projection, declining to 29% in 2003 and 38% for each of the three remaining years.

WatchGuard used a 25% discount rate for valuing the acquired IPR&D. In arriving at the discount rate, WatchGuard considered the implied rate of the transaction and the weighted average cost of capital. WatchGuard also took into account risks related to the characteristics and applications of each project, existing future markets and assessments of the life cycles of each project.

Deferred compensation. A total of approximately \$558,000 of deferred stock-based compensation was recorded in connection with the acquisition. Approximately \$419,000 of the deferred stock-based compensation was due to WatchGuard's assumption of unvested options to purchase RapidStream common stock. This deferred stock-based compensation was based on the intrinsic value of the unvested options at the closing date of the merger. In addition, before the close of the merger, twelve RapidStream employees were allowed to exercise a portion of their unvested options. The WatchGuard stock that was acquired by the former RapidStream employees in exchange for the RapidStream stock acquired upon the exercise of these options is considered restricted and the restrictions will lapse over the original vesting term of the options, which did not exceed 28 months from the date of purchase. Additionally, because the shares of RapidStream were exchanged for a cash payment in addition to shares of WatchGuard common stock, the cash payment related to the restricted shares is also subject to the same vesting period. The total number of restricted shares is 25,281 and the intrinsic value of the arrangement in the amount of \$139,000 is recorded as deferred compensation, based on the fair value of WatchGuard common stock on the closing date of the merger. At December 31, 2002, 8,821 of these shares remained subject to repurchase.

Pro forma results. The following unaudited pro forma combined historical results for 2001 and 2002 are presented as if RapidStream had been acquired on January 1, 2001 and 2002. The pro forma results, which exclude the nonrecurring charge in 2002 of \$1.2 million for IPR&D, are presented below (in thousands, except per share data):

	Years Ended December 31,	
	2001	2002
Total revenues, net	\$ 66,094	\$ 76,174
Net loss	\$(56,586)	\$(35,776)
Pro forma basic and diluted net loss per share	\$ (1.79)	\$ (1.00)

Qiave Technologies Corporation

In October 2000, WatchGuard acquired Qiave Technologies Corporation. The total consideration paid for Qiave was approximately \$70.0 million, including approximately \$400,000 in direct acquisition costs, and was comprised of 1,292,997 shares of WatchGuard common stock valued at \$64.6 million, including 299,495 shares

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

that were subject to repurchase by WatchGuard, and the assumption of options to purchase 100,856 shares of WatchGuard common stock with a fair value of \$5.0 million. WatchGuard accounted for the acquisition using the purchase method of accounting. The results of operations of Qiave and the fair value of assets acquired have been included in the consolidated financial statements beginning on the acquisition date.

The aggregate purchase price was allocated based on estimated fair values on the acquisition date and excludes \$19.3 million in consideration related to deferred stock-based compensation for common stock subject to repurchase and assumption of unvested options to purchase common stock, as follows (in thousands):

Fair value of Qiave tangible assets, net of current liabilities	\$ 654
Intangible assets:	
Acquired workforce	592
Current technology	13,351
Goodwill	<u>31,707</u>
Total intangibles	45,650
Acquired in-process research and development	<u>4,399</u>
Total purchase price	50,703
Deferred stock-based compensation	<u>19,342</u>
Total consideration, including deferred stock-based compensation	<u>\$70,045</u>

Acquired workforce. The value assigned to the workforce in place was determined using the avoided cost approach. Under this approach, the workforce is valued according to the costs WatchGuard avoided by obtaining a pre-existing, trained and fully efficient team rather than assembling a workforce. On January 1, 2002, in accordance with the newly adopted SFAS No. 142, "Goodwill and Other Intangible Assets," the remaining unamortized balance of an assembled workforce intangible asset of \$345,000 was reclassified to goodwill.

Current technology. Values assigned to the developed technology were determined using the income approach. Under the income approach, fair value reflects the present value of the projected earnings that are expected to be generated by the current technology. To determine the value of the developed technology, WatchGuard discounted the expected future cash flows of the existing technology products at a rate of 25%, taking into account risks related to the characteristics and applications of each product, existing and future markets, and assessments of the life-cycle stage of each project. Based on this analysis, WatchGuard capitalized the existing technology that had reached technological feasibility. The projected revenues used in the income approach were based on estimates of potential future revenues that WatchGuard believed were likely be generated by the commercial sales of the technology. During the fourth quarter of 2002 WatchGuard developed a business plan that, because of limited resources, de-emphasized further development and integration of the technology acquired from Qiave. Separately, WatchGuard continued to realize lower than expected revenue from products based on Qiave technology. In accordance with SFAS No. 144, "Accounting for the Impairment or Disposal of Long-Lived Assets," the discounted expected future cash flows were determined to be insufficient to support the carrying value of the Qiave capitalized technology. WatchGuard therefore recorded an impairment charge of \$6.7 million of capitalized technology related to the acquisition of Qiave. The corresponding increase in accumulated amortization leaves a net balance of \$186,000.

Acquired in-process research and development. Values assigned to IPR&D were determined using an income approach. To determine the value of the IPR&D, WatchGuard considered, among other factors, the state of development of each project, the time and cost needed to complete each project, expected income and associated risks, which included the inherent difficulties and uncertainties in completing the project and achieving technological feasibility and risks related to the viability of and potential changes in future target

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

markets. This analysis resulted in amounts assigned to IPR&D projects that had not yet reached technological feasibility and do not have alternative future uses. The entire \$4.4 million allocated to acquired IPR&D was expensed on the date of acquisition.

At the time of the acquisition, six IPR&D projects were identified as being related to future products for which technological or commercial feasibility had not yet been established and that did not have an alternative future use. WatchGuard analyzed each project, using estimated percentage completion factors ranging from 10% to 85%. Revenue attributable to Qiave's IPR&D was assumed to increase after each of the first three years of a five-year projection period after the year of introduction, at annual rates ranging from 60% to 216%, decreasing to a 27% growth rate in revenues after the fourth year in the projection. Projected annual revenues related to in-process technology ranged from approximately \$1.1 million to \$14.8 million over the term of the projections. These projections were based on aggregate revenue growth rates for the business as a whole, anticipated growth rates for the global Internet security market, anticipated product development and product introduction cycles and the estimated life of the underlying technology.

Gross profit was assumed to remain at 93% of revenues for each of the five years of the projection period. Operating expenses, including sales and marketing, research and development and general and administrative costs, were assumed to be 48% of revenues in the initial year of the projection, declining to 44% for each of the four remaining years.

WatchGuard used a 35% discount rate for valuing the acquired IPR&D. In arriving at the discount rate, WatchGuard considered the implied rate of the transaction and the weighted average cost of capital. WatchGuard also took into account risks related to the characteristics and applications of each project, existing future markets, and assessments of the life cycles of each project.

The unaudited pro forma combined historical results, presented as if Qiave had been acquired on January 1, 2000 and excluding the nonrecurring charge for IPR&D in 2000, are presented below. Pro forma results for 1999 are not presented because Qiave had no significant operations in 1999 (in thousands):

	December 31, 2000
Total revenues, net	\$ 60,703
Net loss	\$(29,536)
Pro forma net loss per share	\$ (1.21)

Deferred stock-based compensation. In connection with employment agreements and related stock retention agreements with four of Qiave's key employees, 299,495 shares of WatchGuard common stock otherwise issuable to these employees pursuant to the acquisition agreement are subject to repurchase and were released from the repurchase restriction over a two-year vesting period. The value of these shares has been recorded as \$15.0 million in deferred stock-based compensation, based on the fair value of WatchGuard common stock on the closing date of the Qiave acquisition, and was amortized over a two-year vesting period using a graded vesting approach. At December 31, 2002 there were no shares remaining subject to repurchase. In addition, options to purchase shares of Qiave common stock that were outstanding at the time of the merger were assumed by WatchGuard and converted into options to purchase 100,856 shares of WatchGuard common stock. Deferred stock-based compensation originating from the assumption of Qiave stock options was \$4.3 million.

12. Business Restructuring

During 2002, WatchGuard recorded restructuring charges of approximately \$8.1 million. Approximately \$6.7 million of these charges relates to the 2002 restructuring plan and \$1.4 million relates to revised estimates under the 2001 restructuring plan.

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

2001 Restructuring

In the second quarter of 2001, WatchGuard announced a restructuring plan designed to streamline operations and reduce operating costs. This restructuring plan included a reduction in workforce and a consolidation of excess facilities, in addition to other cost-saving strategies. As part of the restructuring plan, WatchGuard exited the consumer security market and terminated various original equipment manufacturer agreements to develop product and services for that market, and streamlined operations in support of new products and services aimed at business customers. As a result of this restructuring, WatchGuard recorded a \$2.9 million restructuring charge in the quarter ended June 30, 2001. Additional charges of \$820,000, \$524,000 and \$859,000 were recorded related to the restructuring during the quarters ended December 31, 2001, June 30, 2002 and December 2002, respectively. The additional restructuring costs recorded in 2002 relate to revised estimates of the costs associated with the consolidation and sublease of excess facilities.

As part of this reorganization, WatchGuard implemented a workforce reduction of 50 employees, which represented approximately 16% of WatchGuard's employee base at that time and included employees from all of WatchGuard's functional areas. All such employees were terminated prior to June 30, 2001. Other expenses associated with the reorganization consisted of stock-based compensation expense associated with the acceleration of vesting of stock subject to repurchase and stock options held by terminated employees, the discontinuation of the consumer security market products and the abandonment of facilities and equipment. Costs that related to ongoing operations were not included as restructuring charges. All restructuring charges have been paid as of December 31, 2002, except accrued amounts primarily related to losses for the lease buyout or sublease of abandoned facilities, which are expected to be realized through August 2010. Revenues recorded from the consumer security market were insignificant prior to the restructuring. The accrued liability relating to this restructuring as of December 31, 2001 and 2002 and activity recorded through 2001 and 2002 is as follows (in thousands):

	Restructuring Charges in 2001	Amounts Paid or Charged in 2001	December 31, 2001 Accrued Restructuring Balance
Severance and termination benefits	\$1,015	\$(1,015)	\$ —
Stock-based compensation	579	(579)	—
Abandoned facilities and other	2,126	(640)	1,486
Total	\$3,720	\$(2,234)	\$1,486

	Restructuring Charges in 2002	Amounts Paid or Charged in 2002	December 31, 2002 Accrued Restructuring Balance
Abandoned facilities and other	\$1,383	\$(834)	\$2,035

2002 Restructuring

In the second quarter of 2002, WatchGuard implemented a restructuring plan primarily designed to eliminate redundancies and excess headcount resulting from the acquisition of RapidStream (see Note 11), which included a reduction in workforce, consolidation of excess facilities and elimination of technology-related contracts that are no longer required or part of WatchGuard's strategy. As a result of this restructuring, WatchGuard recorded a \$3.7 million restructuring charge during the second quarter of 2002 and an additional charge of \$3 million during the fourth quarter of 2002. The upward revision of restructuring losses in the fourth

WATCHGUARD TECHNOLOGIES, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS—(Continued)

quarter of 2002 is due to continued poor real estate market conditions in the areas where these excess facilities are located.

The restructuring charge for 2002 included the following (in thousands):

	Restructuring Charges in 2002	Amounts Paid or Charged in 2002	December 31, 2002 Accrued Restructuring Balance
Severance and termination benefits	\$ 529	\$ (529)	\$ —
Costs related to cancellation of technology-related contracts	637	(57)	580
Abandoned facilities and other	<u>5,542</u>	<u>(750)</u>	<u>4,792</u>
Total	<u>\$6,708</u>	<u>\$(1,336)</u>	<u>\$5,372</u>

As part of this reorganization, WatchGuard implemented a workforce reduction of 36 employees, which represented approximately 10% of WatchGuard's post-acquisition employee base and included employees from all of WatchGuard's functional areas. All such employees were terminated prior to June 30, 2002. Other costs associated with the reorganization consist of contract terminations and the consolidation of excess facilities. Costs that related to ongoing operations were not included as restructuring charges. Restructuring charges for severance and termination benefits were paid by December 31, 2002, while accrued amounts related to losses for the lease buyout or sublease of abandoned facilities of approximately \$4.8 million at December 31, 2002 are expected to be realized through 2010. Accrued costs of technology contracts will be paid in the first quarter of 2003.

SCHEDULE II
VALUATION AND QUALIFYING ACCOUNTS
(In thousands)

Column A	Column B	Column C	Column D	Column E	Column F
Description	Balance at Beginning of Period	Charged to Revenue, Costs or Expenses	Charged to Other Accounts —Describe	Deductions —Describe	Balance at End of Period
Year ended December 31, 2000					
Allowance for uncollectible accounts	\$ 177	\$ 546	\$ —	\$ 90(A)	\$ 633
Sales return reserve and allowances	\$ 550	\$1,932	\$ —	\$1,517(B)	\$ 965
Inventory reserve	\$ 69	\$ 430	\$ —	\$ 54(C)	\$ 445
Year ended December 31, 2001					
Allowance for uncollectible accounts	\$ 633	\$ 831	\$ —	\$ 671(A)	\$ 793
Sales return reserve	\$ 965	\$6,924	\$ —	\$5,845(B)	\$2,046
Inventory reserve and allowances	\$ 445	\$1,291	\$ —	\$1,388(C)	\$ 348
Year ended December 31, 2002					
Allowance for uncollectible accounts	\$ 793	\$ (75)	\$ —	\$ 232(A)	\$ 486
Sales return reserve and allowances	\$2,046	\$4,601	\$ —	\$4,802(B)	\$1,845
Inventory reserve	\$ 348	\$1,027	\$ —	\$ 750(C)	\$ 625

(A) Deductions consist of write-offs of uncollectible accounts.

(B) Deductions consist of product returns, price protection credits issued and credits issued under promotional allowances previously accrued.

(C) Deductions consist of write-offs of obsolete or excess quantities of inventory.

ITEM 9. CHANGES AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURE

None.

PART III

ITEM 10. DIRECTORS AND EXECUTIVE OFFICERS OF THE REGISTRANT

(a) The information regarding our directors required by this item is incorporated into this annual report by reference to the section entitled "Election of Directors" in the proxy statement for our annual meeting of stockholders to be held on May 22, 2003.

(b) The information regarding our executive officers required by this item is incorporated into this annual report by reference to the section entitled "Executive Officers" in the proxy statement for our annual meeting of stockholders to be held on May 22, 2003.

We will file the proxy statement for our 2003 annual meeting of stockholders within 120 days of December 31, 2002, our fiscal year end.

ITEM 11. EXECUTIVE COMPENSATION

The information regarding executive compensation required by this item is incorporated into this annual report by reference to the section entitled "Executive Compensation" in the proxy statement for our annual meeting of stockholders to be held on May 22, 2003. We will file the proxy statement for our 2003 annual meeting of stockholders within 120 days of December 31, 2002, our fiscal year end.

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT

The information regarding beneficial ownership of our common stock required by this item is incorporated into this annual report by reference to the section entitled "Security Ownership of Certain Beneficial Owners and Management" and "Securities Authorized for Issuance Under Equity Compensation Plans" in the proxy statement for our annual meeting of stockholders to be held on May 22, 2003. We will file the proxy statement within 120 days of December 31, 2002, our fiscal year end.

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS

The information regarding certain relationships and related transactions required by this item is incorporated into this annual report by reference to the section entitled "Certain Relationships and Related Transactions" in the proxy statement for our annual meeting of stockholders to be held on May 22, 2003. We will file the proxy statement within 120 days of December 31, 2002, our fiscal year-end.

ITEM 14. CONTROLS AND PROCEDURES

The term "disclosure controls and procedures" is defined in Rules 13a-14(c) and 15d-14(c) of the Securities Exchange Act of 1934, or the Exchange Act. These rules refer to the controls and other procedures of a company that are designed to ensure that the information required to be disclosed by a company in the reports that it files under the Exchange Act is recorded, processed, summarized and reported within required time periods. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed in our Exchange Act reports is accumulated and communicated to management, including our chief executive officer and chief financial officer, as appropriate to allow timely decisions regarding required disclosure.

Our chief executive officer and our chief financial officer have evaluated the effectiveness of our disclosure controls and procedures as of the Evaluation Date, which is a date within 90 days before the filing of this annual report, and they have concluded that, as of the Evaluation Date, our disclosure controls and procedures were effective.

There were no significant changes to our internal controls or in other factors that could significantly affect our internal controls subsequent to the Evaluation Date.

ITEM 16. PRINCIPAL ACCOUNTANT FEES AND SERVICES

The information regarding principal accountant fees and services required by this item is incorporated into this annual report by reference to the section entitled "Independent Auditors" in the proxy statement for our annual meeting of stockholders to be held on May 22, 2003. We will file the proxy statement within 120 days of December 31, 2002, our fiscal year-end.

PART IV

ITEM 15. EXHIBITS, FINANCIAL STATEMENT SCHEDULES AND REPORTS ON FORM 8-K

(a) Financial Statements and Financial Statement Schedules

(1) Index to Financial Statements

	<u>Page</u>
Report of Ernst & Young LLP, Independent Auditors	57
Consolidated Balance Sheets	58
Consolidated Statements of Operations	59
Consolidated Statements of Stockholders' Equity	60
Consolidated Statements of Cash Flows	61
Notes to Consolidated Financial Statements	62

(2) Index to Financial Statement Schedules

Schedule II—Valuation and Qualifying Accounts for each of the three years ended December 31, 2002, 2001 and 2000.

Schedules not listed above have been omitted because they are not applicable or are not required or the information required to be set forth in the schedules is included in the consolidated financial statements or related notes.

(3) Exhibits

<u>Number</u>	<u>Description</u>
2.1†	Agreement and Plan of Merger dated as of February 6, 2002, among River Acquisition Corp., RapidStream, Inc., the registrant, and for purposes of Section 6.16 only, certain management shareholders of RapidStream, Inc. (Exhibit 2.1) (A)
2.2	Amendment No. 1 to Agreement and Plan of Merger dated as of March 1, 2002, by and among the registrant, River Acquisition Corp., RapidStream, Inc. and Wai San Loke, as Shareholder Representative (Exhibit 2.2) (B)
3.1	Restated Certificate of Incorporation of the registrant (Exhibit 3.1) (C)
3.2	Restated Bylaws of the registrant (Exhibit 3.2) (C)
10.1	Lease Agreement, dated as of March 1, 2000, between 505 Union Station and the registrant (Exhibit 10.1) (D)
10.2	1996 Stock Incentive Compensation Plan (Exhibit 10.6) (C)
10.3	2000 Stock Option Plan (Exhibit 10.1) (E)
10.4	1998 RapidStream, Inc. Stock Option Plan (Exhibit 10.1) (F)
10.5	Qiave Technologies Corporation 2000 Stock Option Plan (Exhibit 99.1) (G)
10.6	1999 Employee Stock Purchase Plan (Exhibit 10.10) (C)
10.7	Standardized Adoption Agreement Prototype Cash or Deferred Profit-Sharing Plan and Trust (401(k) plan), effective as of September 1, 1998 (Exhibit 10.7) (C)
10.8	Shareholders Agreement, dated as of February 6, 2002, by and among River Acquisition Corp., RapidStream, Inc., certain shareholders of RapidStream, Inc. and the registrant (Exhibit 10.1) (A)
10.9	Escrow Agreement, dated as of April 2, 2002, by and between the registrant, RapidStream, Inc., Wai San Loke, as Shareholder Representative, and Mellon Investor Services LLC, as escrow agent (Exhibit 10.2) (B)

<u>Number</u>	<u>Description</u>
10.10	Offer letter to Jim Cady, dated as of July 1, 2001 (Exhibit 10.1) (H)
10.11	Offer letter to Gary J. Franza, dated as of July 3, 2001 (Exhibit 10.1) (I)
10.12	Offer letter to Jean Nassar, dated as of November 3, 2001 (Exhibit 10.2) (I)
21.1	Subsidiaries of the registrant
23.1	Consent of Ernst & Young LLP, Independent Auditors
99.1	Certification of Chief Executive Officer
99.2	Certification of Chief Financial Officer

† Portions of this exhibit have been omitted based on a request for confidential treatment filed with the SEC. The omitted portions of the exhibits have been filed separately with the SEC.

- (A) Incorporated by reference to the specified exhibit to the registrant's Current Report on Form 8-K (File No. 000-26819), filed with the SEC on February 15, 2002.
- (B) Incorporated by reference to the specified exhibit to the registrant's Current Report on Form 8-K (File No. 000-26819), filed with the SEC on April 12, 2002.
- (C) Incorporated by reference to the specified exhibit to the registrant's Registration Statement on Form S-1 (File No. 333-76587), filed with the SEC on April 20, 1999, as amended.
- (D) Incorporated by reference to the specified exhibit to the registrant's Annual Report on Form 10-K/A (File No. 000-26819), filed with the SEC on May 1, 2000.
- (E) Incorporated by reference to the specified exhibit to the registrant's Quarterly Report on Form 10-Q for the quarter ended March 31, 2001 (File No. 000-26819), filed with the SEC on May 15, 2001.
- (F) Incorporated by reference to the specified exhibit to the registrant's Registration Statement on Form S-8 (File No. 333-86168), filed with the SEC on April 12, 2002.
- (G) Incorporated by reference to the specified exhibit to the registrant's Registration Statement on Form S-8 (File No. 333-51196), filed with the SEC on December 4, 2000.
- (H) Incorporated by reference to the specified exhibit to the registrant's Quarterly Report on Form 10-Q for the quarter ended June 30, 2001 (File No. 000-26819), filed with the SEC on August 13, 2001.
- (I) Incorporated by reference to the specified exhibit to the registrant's Quarterly Report on Form 10-Q for the quarter ended March 31, 2002 (File No. 000-26819), filed with the SEC on May 15, 2002.

(b) Reports on Form 8-K

We filed a current report on Form 8-K on October 25, 2002 to announce that our board of directors had approved the repurchase by WatchGuard of up to \$8 million of WatchGuard common stock.

SIGNATURES

Pursuant to the requirements of Section 13 or 15(d) of the Securities Exchange Act of 1934, as amended, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized, in the city of Seattle, state of Washington, on March 26, 2003.

WATCHGUARD TECHNOLOGIES, INC.

By: /s/ JAMES A. CADY
 James A. Cady
 President and Chief Executive Officer

POWER OF ATTORNEY

Each person whose individual signature appears below hereby authorizes and appoints James A. Cady and Steven N. Moore, and each of them, with full power of substitution and resubstitution and full power to act without the other, as his true and lawful attorney-in-fact and agent to act in his name, place and stead and to execute in the name and on behalf of each person, individually and in each capacity stated below, and to file, any and all amendments to this report, and to file the same, with all exhibits thereto, and other documents in connection therewith, with the Securities and Exchange Commission, granting unto said attorneys-in-fact and agents, and each of them, full power and authority to do and perform each and every act and thing, ratifying and confirming all that said attorneys-in-fact and agents or any of them or their or his substitute or substitutes may lawfully do or cause to be done by virtue thereof.

Pursuant to the requirements of the Securities Act of 1934, as amended, this report has been signed by the following persons, on behalf of the registrant, in the capacities and on the dates indicated.

<u>Signature</u>	<u>Title</u>	<u>Date</u>
/s/ JAMES A. CADY James A. Cady	President, Chief Executive Officer and Chairman of the Board (Principal Executive Officer)	March 26, 2003
/s/ MICHAEL E. MCCONNELL Michael E. McConnell	Senior Vice President, Chief Financial Officer and Treasurer (Principal Financial and Accounting Officer)	March 26, 2003
/s/ MICHAEL R. HALLMAN Michael R. Hallman	Director	March 26, 2003
/s/ STEVEN N. MOORE Steven N. Moore	Director	March 26, 2003
/s/ WILLIAM J. SCHROEDER William J. Schroeder	Director	March 26, 2003
/s/ JOHN J. TODD John J. Todd	Lead Director	March 25, 2003
/s/ CHARLES P. WAITE, JR. Charles P. Waite, Jr.	Director	March 26, 2003

CERTIFICATIONS

I, James A. Cady, certify that:

1. I have reviewed this annual report on Form 10-K of WatchGuard Technologies, Inc. ("WatchGuard");
2. Based on my knowledge, this annual report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this annual report;
3. Based on my knowledge, the financial statements, and other financial information included in this annual report, fairly present in all material respects the financial condition, results of operations and cash flows of WatchGuard as of, and for, the periods presented in this annual report;
4. WatchGuard's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-14 and 15d-14) for WatchGuard and we have:
 - a) designed such disclosure controls and procedures to ensure that material information relating to WatchGuard, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this annual report is being prepared;
 - b) evaluated the effectiveness of WatchGuard's disclosure controls and procedures as of a date within 90 days prior to the filing date of this annual report (the "Evaluation Date"); and
 - c) presented in this annual report our conclusions about the effectiveness of the disclosure controls and procedures based on our evaluation as of the Evaluation Date;
5. WatchGuard's other certifying officer and I have disclosed, based on our most recent evaluation, to WatchGuard's auditors and the audit committee of WatchGuard's board of directors (or persons performing the equivalent function):
 - a) all significant deficiencies in the design or operation of internal controls which could adversely affect WatchGuard's ability to record, process, summarize and report financial data and have identified for WatchGuard's auditors any material weaknesses in internal controls; and
 - b) any fraud, whether or not material, that involves management or other employees who have a significant role in WatchGuard's internal controls; and
6. WatchGuard's other certifying officer and I have indicated in this annual report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of our most recent evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

Date: March 26, 2003

/s/ JAMES A. CADY

James A. Cady
President, Chief Executive Officer and
Chairman of the Board

I, Michael E. McConnell, certify that:

1. I have reviewed this annual report on Form 10-K of WatchGuard Technologies, Inc. ("WatchGuard");
2. Based on my knowledge, this annual report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this annual report;
3. Based on my knowledge, the financial statements, and other financial information included in this annual report, fairly present in all material respects the financial condition, results of operations and cash flows of WatchGuard as of, and for, the periods presented in this annual report;
4. WatchGuard's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-14 and 15d-14) for WatchGuard and we have:
 - a) designed such disclosure controls and procedures to ensure that material information relating to WatchGuard, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this annual report is being prepared;
 - b) evaluated the effectiveness of WatchGuard's disclosure controls and procedures as of a date within 90 days prior to the filing date of this annual report (the "Evaluation Date"); and
 - c) presented in this annual report our conclusions about the effectiveness of the disclosure controls and procedures based on our evaluation as of the Evaluation Date;
5. WatchGuard's other certifying officer and I have disclosed, based on our most recent evaluation, to WatchGuard's auditors and the audit committee of WatchGuard's board of directors (or persons performing the equivalent function):
 - a) all significant deficiencies in the design or operation of internal controls which could adversely affect WatchGuard's ability to record, process, summarize and report financial data and have identified for WatchGuard's auditors any material weaknesses in internal controls; and
 - b) any fraud, whether or not material, that involves management or other employees who have a significant role in WatchGuard's internal controls; and
6. WatchGuard's other certifying officer and I have indicated in this annual report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of our most recent evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

Date: March 26, 2003

/s/ MICHAEL E. MCCONNELL

Michael E. McConnell
Senior Vice President, Chief Financial
Officer and Treasurer

Directors

James A. Cady

Chairman, President and CEO
WatchGuard Technologies, Inc.

Steven N. Moore

Executive Vice President and Secretary
WatchGuard Technologies, Inc.

Michael R. Hallman

President
The Hallman Group

Ellen M. Hancock

Former Chairman and Chief Executive Officer
Exodus Communications

Michael R. Kourey

Chief Financial Officer
Polycom, Inc.

Richard A. LeFavre, Ph. D.

Executive Director
William J. von Liebig Center
for Entrepreneurism and Technology
Advancement, UC San Diego

William J. Schroeder

President and CEO
Vormetric, Inc.

John J. Todd

President and CEO
APEX

Charles P. Waite, Jr.*

General Partner
OVP Venture Partners

Executive Management

James A. Cady

Chairman, President and CEO

Steven N. Moore

Executive Vice President and Secretary

Michael E. McConnell

Senior Vice President, CFO and Treasurer

Gary M. Franza

Senior Vice President, Worldwide Sales

Jean E. Nassar

Senior Vice President, Marketing

Mark W. Stevens

Senior Vice President, Network Security

Janice L. Clusserath

Vice President, Human Resources

John S. Stuckey

Vice President, RapidStream

Patrick E. Weston

Vice President, Engineering

Other Information

Exchange and Symbol

Nasdaq
WGRD

Investor Relations

Miles G. Goda
(206) 613-0826

Legal Counsel

Michael C. Piraino
Vice President and General Counsel

Independent Auditors

Ernst & Young LLP
999 Third Ave.
Seattle, WA 98104

Outside Legal Counsel

Orrick, Herrington & Sutcliffe LLP
719 Second Ave., Suite 900
Seattle, WA 98104

Transfer Agent and Registrar

Mellon Investor Services LLC
85 Challenger Rd., Overpeck Center
Ridgefield Park, NJ 07660
(800) 522-6645

* Mr Waite will resign from WatchGuard's Board of Directors effective as of the 2003 annual meeting of stockholders

Notice of Annual Meeting

The annual meeting of stockholders will be held on June 5, 2003, at 9:00am at the Grand Hyatt Seattle, 721 Pine St., Seattle, WA 98101.

Corporate Headquarters

505 Fifth Ave. S., Suite 500
Seattle, WA 98104-3892
(206) 521-8340

About WatchGuard

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.

Copyright Information

©2003 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, RapidStream, LiveSecurity, Firebox, ServerLock, and AppLock are either registered trademarks or trademarks of WatchGuard Technologies, Inc. or its subsidiaries in the United States and/or other countries. Check Point is a trademark of Check Point Software Technologies Ltd.

Certain statements in this Annual Report, including statements about possible or expected future operating results, trends in financial results and business plans, including those related to revenue growth and earnings growth, statements about future technology plans and products and other statements about our plans, objectives, intentions, and expectations are "forward-looking statements" within the meaning of the Securities Act of 1933, as amended. Forward-looking statements are based on the opinions and estimates of management at the time the statements are made and are subject to known and unknown risks and uncertainties and inaccurate assumptions that could cause actual results to differ materially from those expected or implied by the forward-looking statements. Our actual results could differ materially from those anticipated in the forward-looking statements for many reasons, including the risk that our future operating results will fall below expectations, the risk that future technology plans or products will be delayed or canceled and the other risks described under "Important Factors That May Affect Our Operating Results, Our Business and Our Stock Price" in our annual report on Form 10-K for the year ended December 31, 2002 included in this Annual Report, and in our Securities and Exchange Commission filings from time to time. Readers are cautioned not to place undue reliance upon these forward-looking statements, which speak only as of the date of this report.



