SOURCEFIRE INC
Form 10-K
February 28, 2008

UNITED STATES SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

Form 10-K

(Mark One)

þ	**ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 FOR THE FISCAL YEAR ENDED DECEMBER 31, 2007**
o	**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 1-33350

SOURCEFIRE, INC.
(Exact name of Registrant as Specified in its Charter)

Delaware *(State or Other Jurisdiction of Incorporation or Organization)*	**52-2289365** *(I.R.S. Employer Identification No.)*
9770 Patuxent Woods Drive **Columbia, Maryland** *(Address of Principal Executive Offices)*	**21046** *(Zip Code)*

Registrant s telephone number, including area code:
(410) 290-1616

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

Title of Each Class	**Name of Exchange on Which Registered**
Common Stock, $0.001 par value	Nasdaq Global Market

Securities registered pursuant to Section 12(g) of the Act: none

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes o   No þ

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes o   No þ

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 þ   No o

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. þ

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See definitions of large accelerated filer,   accelerated filer, and smaller reporting company in Rule 12b-2 of the Exchange Act. (Check one):

Large Accelerated Filer o	Accelerated Filer o
Non-Accelerated Filer þ (Do not check if smaller reporting company)	Smaller reporting Company o

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes o   No þ

As of June 30, 2007, there were 24,108,428 shares of the registrant s Common Stock outstanding. The aggregate market value of such shares held by non-affiliates of the registrant, based upon the closing sale price ($13.99) of such shares on the Nasdaq Global Market for such date, was approximately $183.4 million.

As of February 25, 2008, there were outstanding 24,647,719 shares of the registrant s Common Stock.

DOCUMENTS INCORPORATED BY REFERENCE

Certain portions of the definitive Proxy Statement to be used in connection with the registrant s 2008 Annual Meeting of Stockholders are incorporated by reference into Part III of this Form 10-K to the extent stated. That Proxy Statement will be filed within 120 days of registrant s fiscal year ended December 31, 2007.

SOURCEFIRE, INC.

ANNUAL REPORT ON FORM 10-K
FOR THE YEAR ENDED DECEMBER 31, 2007

TABLE OF CONTENTS

PART I

PART II

PART III

PART IV

References in this Annual Report on Form 10-K to Sourcefire, we, us , our or the Company refer to Sourcefire, I and its subsidiaries, taken as a whole, unless a statement specifically refers to Sourcefire, Inc.

FORWARD-LOOKING STATEMENTS

This annual report contains both historical and forward-looking statements. All statements other than statements of historical fact are, or may be deemed to be, forward-looking statements. For example, statements concerning projections, predictions, expectations, estimates or forecasts and statements that describe our objectives, plans or goals are or may be forward-looking statements. These forward-looking statements reflect management s current expectations concerning future results and events and generally can be identified by use of expressions such as may, will, should, could, would, predict, potential, continue, expect, anticipate, future, intend, plar estimate, and similar expressions, as well as statements in future tense. These forward-looking statements include, but are not limited to, the following:

expected growth in the markets for network security products;

our plans to continue to invest in and develop innovative technology and products for our existing markets and other network security markets;

the timing of expected introductions of new or enhanced products;

our expectation of growth in our customer base and increasing sales to existing customers;

our plans to increase revenue through more relationships with original equipment manufacturers, resellers, distributors, government suppliers and co-marketers;

our plans to grow international sales;

our plans to acquire and integrate new businesses and technologies;

our plans to hire more network security professionals and broaden our knowledge base; and

our plans to hire additional sales personnel and the additional revenue we expect them to generate.

The forward-looking statements included in this annual report are made only as of the date of this annual report. We expressly disclaim any intent or obligation to update any forward-looking statements to reflect subsequent events or circumstances. Forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause our actual results, performance or achievements to be different from any future results, performance and achievements expressed or implied by these statements. These risks and uncertainties include, but are not limited to, those discussed in Item 1A. Risk Factors of this annual report.

We operate in an industry in which it is difficult to obtain precise industry and market information. Although we have obtained some industry data from outside sources that we believe to be reliable, in certain cases we have based certain statements contained in this annual report regarding our industry and our position in the industry on our estimates concerning, among other things, our customers and competitors. These estimates are based on our experience in the industry, conversations with our principal suppliers and customers and our own investigations of market conditions. The statistical data contained in this annual report regarding the network security software industry are our statements, which are based on data we obtained from industry sources.

SOURCEFIRE®, SNORT®, the Sourcefire logo, the Snort and Pig logo, SECURITY FOR THE REAL WORLDtm, SOURCEFIRE DEFENSE CENTERtm, SOURCEFIRE 3Dtm, RNAtm, ClamAVtm and certain other trademarks and logos are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries. This annual report also refers to the products or services of other companies or persons by the trademarks and trade names used and owned by those companies or persons.

PART I

BUSINESS

Item 1. *BUSINESS*

Overview

We are a leading provider of Enterprise Threat Management (ETM) solutions for information technology (IT) infrastructures of commercial enterprises (e.g., healthcare, financial services, manufacturing, energy, education, retail, telecommunications) and federal and state government organizations. The Sourcefire 3D^{tm} System comprised of multiple Sourcefire hardware and software product offerings provides a comprehensive, intelligent network defense that unifies intrusion prevention system (IPS), network behavior analysis (NBA), network access control (NAC) and vulnerability assessment (VA) solutions under a common management framework. This ETM approach equips our customers with an efficient and effective layered security defense protecting computer network assets before, during and after an attack.

Since 2001, Sourcefire has garnered a reputation in the network security industry of being a staunch advocate for open source. Over the years, this has developed into a key competitive distinction for Sourcefire as we now manage two of the security industry s leading open source initiatives, Snort® and ClamAV^{tm}, in addition to two new open source or freely available entrants, OfficeCat^{tm} and Daemonlogger^{tm}. First published in 1998 by Sourcefire founder and Chief Technology Officer, Martin Roesch, open source Snort has rapidly become the de facto standard for intrusion detection and prevention. With over 170,000 registered users, 3 million downloads, and embraced by more than 100 network security providers, more organizations use Snort than any other IPS engine in the world. Further, open source ClamAV is a widely successful anti-malware engine and is most commonly used for email scanning on mail servers. Established in 2001 and acquired by Sourcefire in 2007, the ClamAV malware database incorporates more than 200,000 signatures, downloaded by more than 1 million unique IP addresses per day from more than 130 mirror sites in 44 countries.

Sourcefire embraces open source security as a foundation, but extends that foundation by adding enterprise-class manageability, scalability, and performance. Many Sourcefire 3D System customers, for example, start out using open source Snort, but graduate to Sourcefire s commercial offerings to gain more efficient and effective network security capabilities. By incorporating open source security as a foundation in Sourcefire s commercial product offerings, Sourcefire can:

Seed the market by offering high quality, low cost network security solutions while providing a migration path for customers that require enterprise-class manageability, scalability and performance.

Ensure product quality as many eyes inspect the open code base that forms the foundation for Sourcefire commercial product offerings.

Maximize protection as Snort rules and ClamAV signatures are provided by Sourcefire and a variety of third-party sources, and customers can create their own custom rules and signatures.

Embrace a community of open source evangelists willing to contribute time and effort in inspecting, evaluating, and ultimately using Sourcefire s open source security solutions.

Sourcefire sells its network security solutions to a diverse customer base that includes 29 of the Fortune 100 companies and over half of the 30 largest U.S. government agencies. For the years ended December 31, 2007, 2006 and 2005, we generated approximately 75%, 81% and 82% of our revenue from customers in the United States and 25%, 19% and 18% from customers outside of the United States, respectively. We have expanded our international and indirect distribution channels and, in the future, we expect to increase sales outside of the United States and to source additional customer prospects and generate an increasing portion of product revenues through alliances with original equipment manufacturers, or OEMs, such as Nokia, Inc. We increased our total revenue from $44.9 million in 2006 to $55.9 million in 2007, representing a growth rate of 24%. For the year ended December 31, 2007, product revenue represented 61% and services revenue represented 39% of our total revenue. We manage our operations on a consolidated basis for purposes of assessing performance and making operating decisions. Accordingly, we do not have reportable segments of our business.

2007 Developments

2007 was an eventful year for Sourcefire. We took our company public, we introduced the industry s first-ever Adaptive IPS technology, and we completed our first acquisition. The following is a list of key Sourcefire company developments that occurred in 2007:

January 16th	Sourcefire announced its position as a Leader in Gartner IPS Magic Quadrant report
March 8th	Sourcefire Initial Public Offering
March 22nd	Sourcefire announced exercise of over-allotment option in connection with Initial Public Offering
April 16th	Sourcefire launched Enterprise Threat Management (ETM) strategy
May 2nd	Sourcefire announced Real-time User Awareness (RUA) product
June 26th	Sourcefire added to Russell 3000 Index
July 9th	Sourcefire launched 10Gbps 3D9800 Sensor
August 10th	Sourcefire named Douglas McNitt as General Counsel
August 17th	Sourcefire acquired ClamAV open source network anti-virus project
September 17th	Sourcefire launched 3D System 4.7, including Adaptive IPS and NetFlow Analysis
September 23rd	Sourcefire increased international growth with Australian expansion
October 1st	Sourcefire joined the PCI Security Standards Council
December 12th	Sourcefire announced Certified ClamAV Support

Initial Public Offering

In March 2007, we completed the initial public offering, or IPO, of our common stock in which we sold and issued 6,185,500 shares of our common stock, including 865,500 shares sold by us pursuant to the underwriters full exercise of their over-allotment option, at an issue price of $15.00 per share. We raised a total of $92.8 million in gross proceeds from the IPO, or approximately $83.9 million in net proceeds after deducting underwriting discounts and commissions of $6.5 million and other offering costs of $2.4 million. Upon the closing of the IPO, all shares of convertible preferred stock outstanding automatically converted into an aggregate of 14,302,056 shares of common stock.

Acquisition of ClamAV

In August 2007, we closed on our acquisition of the intellectual property assets of ClamAV, an open source anti-malware project. We paid $3.5 million in cash to the former owners, and deposited an additional $1.0 million in cash into escrow, to be paid to the sellers upon the completion of certain additional source code, which is currently expected to be completed in the first quarter of 2008. We allocated $2.9 million of the purchase price to in-process research and development and allocated the remaining $634,000 to certain marketing-related intangible assets. The amounts allocated to in-process research and development were immediately expensed, as there is no anticipated alternative future use for the acquired technology. As of December 31, 2007, we determined that it was probable that the additional source code would be completed in 2008 and the contingent payment would be made; therefore, the $1.0 million placed into escrow was accrued as a liability and recorded as a compensation expense as the sellers are now our employees and the payment is for services rendered.

Our Industry

We believe, based on our review of various industry sources, that the entire network security industry was an $18.7 billion market in 2006 and is projected to grow to $33.8 billion in 2011, representing a compound annual growth rate of approximately 13%. Our core market, intrusion prevention, was $0.9 billion in 2006 and is projected to grow to $2.0 billion in 2011, representing a compound annual growth rate of 16%. Other addressable markets that we serve, or intend to serve, include network behavior analysis (NBA), network access control (NAC), vulnerability assessment (VA), and unified threat management (UTM). We expect that demand for security solutions will continue to grow as organizations seek to address various growing and evolving security challenges, including:

Greater Sophistication, Severity and Frequency of Network Attacks. The growing use of the Internet as a business tool has required organizations to increase the number of access points to their networks, which has made vast amounts of critical information more vulnerable to attack. Theft of sensitive information for financial gain motivates network attackers, who derive profit through identity theft, credit card fraud, money laundering, extortion, intellectual property theft and other illegal means. These profit-motivated attackers, in contrast to the hobbyist hackers of the past, are employing much more sophisticated tools and techniques to generate profits for themselves and their well-organized and well-financed sponsors. Their attacks are increasingly difficult to detect and their tools often establish footholds on compromised network assets with little or no discernible effect, facilitating future access to the assets and the networks on which they reside.

Increasing Risks from Unknown Vulnerabilities. Vulnerabilities in computer software that are discovered by network attackers before they are discovered by security and software vendors represent a tremendous risk. These uncorrected flaws can leave networks largely defenseless and open to exploitation. According to the CERT Coordination Center (CERT-CC), the trends in the rate of vulnerability disclosure are particularly alarming, with approximately 5,990 vulnerabilities cataloged in 2005 and 8,064 vulnerabilities cataloged in 2006. During 2007, Microsoft alone issued 43 patches designated as critical for its various software products. Many vulnerabilities have existed since the original release of the affected software products some dating back to the 1990s but were not corrected until recently.

Diverse Demands on Security Administrators. The proliferation of targeted security solutions such as firewalls, intrusion prevention systems, URL filters, spam filters and anti-spyware solutions, while critical to enhancing network security, create significant administrative burdens on personnel who must manage numerous disparate technologies that are seldom integrated and often difficult to use. Most network security products require manual, labor intensive incident response and investigation by security administrators, especially when false positive results are generated. Compounding these resource constraint issues, many organizations are increasingly challenged by the loss of key personnel as the demand for security experts has risen dramatically in traditional corporate settings, government agencies and the growing number of start-up security companies.

Increasing Visibility of Negligence Lawsuits. Faced with an ever-growing list of laws and regulations, organizations can no longer plead ignorance when defending corporate negligence lawsuits resulting from internal and external security breaches. Today s enterprises must comply with a series of government and/or industry regulations defining best practices for network security. Achieving compliance with all manner of regulations is a complex and costly issue for nearly every organization.

Heightened Government and Industry Regulation. Rapidly growing government regulation is forcing compliance with increased requirements for network security, which has escalated demand for security solutions that both meet compliance requirements and reduce the burden of compliance reporting and enforcement. Examples of these laws include:

> The Payment Card Industry Data Security Standard, or PCI DSS, which provides guidelines to help organizations that process credit card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats. A company processing, storing, or transmitting payment card data must be PCI DSS compliant or risk losing its ability to process credit card payments.

The Health Insurance Portability and Accountability Act of 1996, or HIPAA, and its related rules, which establish requirements for safeguards to protect the confidentiality, integrity and availability of electronic protected health information.

The Financial Services Modernization Act of 1999, commonly known as the Gramm-Leach-Bliley Act, which includes provisions to protect consumers   personal financial information held by financial institutions.

The Sarbanes-Oxley Act of 2002, which mandates that public companies demonstrate due diligence in the disclosure of financial information and maintain internal controls and procedures for the communication, storage and protection of such data.

The Federal Information Security Management Act, or FISMA, which requires federal agencies, including contractors and other organizations that work with the agencies, to develop, document and implement an agency-wide information security program.

State privacy laws that regulate the privacy of personal information. California s SB1386, for example, requires notification to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Our Products

Sourcefire manufactures a number of open source and commercial security products. Sourcefire s key open source product offerings include:

Snort® The traffic inspection engine used in our intrusion prevention system is the open source technology called Snort. Martin Roesch, our founder and Chief Technology Officer, created Snort in 1998 and assigned his rights to Sourcefire upon its incorporation. Our employees, including Mr. Roesch, have authored all major components of Snort, and we maintain control over the Snort project, including the principal Snort community forum, Snort.org. Snort, which has rapidly become a de facto industry standard for intrusion prevention, has been downloaded over 3 million times. We believe that a majority of the Fortune 100 companies and all of the 30 largest U.S. government agencies use Snort technology to monitor network traffic and that Snort is the most widely deployed intrusion prevention technology worldwide. The ubiquitous nature of the Snort user community represents a significant opportunity to sell our proprietary products to customers that require a complete enterprise solution.

Sourcefire Vulnerability Research Team (VRT) Subscriptions The Sourcefire VRT is a team of experienced network security professionals responsible for writing, testing and publishing Snort rules to defend against both known and zero-day exploits. Snort rules published by the Sourcefire VRT are made available to open source Snort users at no charge on a 30-day delayed basis. Real-time VRT rules updates are made available to Sourcefire commercial IPS customers with an active customer support agreement and to open source Snort users on a subscription basis.

ClamAVtm Founded in 2001, ClamAV is one of the most commonly-used open source anti-malware products in the world. More than one million unique IP addresses download ClamAV updates daily from over 130 mirror servers located in 44 countries. Renowned for its speed and accuracy, ClamAV has been adopted by network security solution and service providers worldwide and is currently integrated within leading enterprise solutions to identify deeply embedded threats such as viruses, trojans, spyware, and other forms of malware. Like Snort, ClamAV s cutting edge security technology is a product of our open source model. In addition to continual innovations to the ClamAV anti-virus engine, the ClamAV core team and ClamAV community deliver daily signature updates to its growing virus database of over 200,000 signatures.

Certified ClamAV Support As with many open source products, support options available to end users have been limited to user mailing lists and message boards. While the community that provides this support is made up of experts who have contributed code and signatures, it does not satisfy the needs of businesses and government agencies that require 24x7 commercial support. This common obstacle to open source adoption is why Sourcefire introduced Certified ClamAV Support. With Certified ClamAV Support, we believe that our customers get the best of both worlds, the hallmark rapid pace of innovation, cost savings and transparency of the open source model combined with the reliable, high quality support provided by a commercial software company.

Sourcefire s commercial hardware and software products are marketed and sold as components of the Sourcefire 3D System. Our 3D System is comprised of the following hardware and software product offerings:

*Sourcefire Defense Center*tm The nerve center of the Sourcefire 3D System, Defense Center unifies critical network security functions including event monitoring, correlation, and prioritization with network and user intelligence for forensic analysis, trends analysis, reporting and alerting. Defense Center is highly extensible, providing application programming interfaces (APIs) to interoperate with a variety of third-party systems (e.g., firewalls, routers, Security Information Event Management, or SIEMs, trouble ticketing and patch management systems). Using Defense Center, customers can control multiple Sourcefire 3D Sensors from a single management console while aggregating and analyzing security and compliance events from across the organization.

Sourcefire 3D^{tm} Sensors   Scaling from 5 Mbps to 10 Gbps, Sourcefire 3D Sensors are highly scalable, fault-tolerant appliances responsible for processing Sourcefire IPS, RNA, RUA and NetFlow Analysis software applications. Sourcefire 3D Sensors are available with a variety of copper and fiber interfaces to meet the connectivity needs of virtually any organization.

Sourcefire IPS^{tm} (Intrusion Prevention System)   Built on the foundation of Snort, Sourcefire IPS uses a rules-based language   a powerful combination of signature-, protocol-, and vulnerability-based inspection methods   to examine network packets for threats. Sourcefire IPS allows users to create, edit, and view detection rules, and full packet payloads are logged for every event so users can see exactly what threatening traffic has been detected. Sourcefire 3D Sensors equipped with Sourcefire IPS software can be placed in passive intrusion detection, or IDS, mode to notify users of incoming threats or in inline IPS mode to block incoming threats.

Sourcefire RNA^{tm} (Real-time Network Awareness)   At the heart of the Sourcefire 3D System is RNA, Sourcefire s network intelligence product that provides persistent visibility into the composition, behavior, topology (the relationship of network components) and risk profile of the network. Network intelligence derived by RNA provides a platform for Defense Center s automated decision-making and network policy compliance enforcement. The ability to continuously discover characteristics and vulnerabilities of virtually any computing device communicating on a network enables Sourcefire IPS to more precisely identify and block threatening traffic and to more efficiently classify threatening and/or suspicious behavior.

Sourcefire RUA^{tm} (Real-time User Awareness)   Sourcefire RUA enables customers to link user identity to security and compliance events. RUA leverages existing investments in Active Directory or Lightweight Directory Access Protocol (LDAP) systems by pairing usernames with host IP addresses involved in security and compliance events. This enables Sourcefire customers to resolve security and compliance events more quickly and easily.

Sourcefire NetFlow Analysis   Sourcefire NetFlow Analysis aggregates data from Cisco routers and switches, thus extending the reach of Sourcefire s network behavior analysis, or NBA, solution to corners of the network where Sourcefire 3D technology has not yet been employed. The combination of RNA and NetFlow data provides customers with the ability to baseline normal network traffic across the enterprise, enabling security analysts to detect suspicious deviations, such as worm propagation, from established baselines. Further, the ability to analyze NetFlow also provides network managers with the network usage intelligence required to identify performance bottlenecks and/or areas of the network where too much bandwidth has been allocated.

Sourcefire Intrusion Agent for Snort   Many Sourcefire commercial customers start out as open source Snort users. To initiate the migration from Snort to the more scalable and manageable Sourcefire 3D System, Sourcefire offers Intrusion Agent software that can be placed on open source Snort Sensors. This enables customers with Defense Center to aggregate and analyze intrusion events from both open source Snort Sensors and commercial Sourcefire 3D Sensors.

Our Services

In addition to our open source and commercial product offerings, we also offer the following services to aid our customers with installing and supporting our ETM solutions:

Sourcefire Customer Support Sourcefire s customer support is designed to ensure customer satisfaction with Sourcefire products. Sourcefire s comprehensive support services include online technical support, over-the-phone support, hardware repair/advanced replacement, and ongoing software updates to Sourcefire products.

Sourcefire Product Services Sourcefire offers a variety of professional services solutions to provide customers with best practices for planning, installing, configuring, and managing all components of the Sourcefire

3D System. The Sourcefire Product Services Team provides customers with individualized, highly concentrated attention that gives organizations a running start and lasting knowledge transfer.

Sourcefire Education & Certification Sourcefire offers a variety of training programs to help security professionals using Sourcefire commercial or open source security solutions get the most out of their investment. Sourcefire training includes instructor-led and custom classes delivered at various locations around the world, onsite at customer premises, and online. In addition, Sourcefire provides a path for interested candidates to distinguish themselves through a certification program. Certification can be achieved on both Sourcefire products and open source Snort, including an expert-level exam for those security professionals who want to obtain certification on both technologies. Through training and testing, certification provides customers and their employees with an understanding of individual skills and experience with Snort and Sourcefire products.

Our Competitive Strengths

We are a leading provider of intelligence driven, open source network security solutions that enable our customers to protect their computer networks in an effective, efficient and highly automated manner. We apply the Sourcefire 3D Systems solution Discover, Determine, Defend to network security through our comprehensive family of integrated products. Our competitive strengths include:

Real-Time Approach to Network Security. Our approach to network security enables our customers to secure their networks by providing real-time defense against both known and unknown threats. Our solution is designed to support a continuum of network security functions that span pre-attack hardening of assets, high fidelity attack identification and disruption and real-time compromise detection and incident response. In addition, our ability to confidently classify and prioritize threats in network traffic and determine the composition, behavior and relationships of network devices, or endpoints, allows us to reliably automate what are otherwise manual, time-intensive processes. For example, our 3D Sensor may trigger an alert upon identifying a Microsoft Windows-specific threat. The Defense Center would collect this alert, or security event, and classify and prioritize the event based upon a number of factors, including whether any other 3D Sensor generated the same alert, whether the network endpoints are vulnerable to that specific attack based on intelligence collected by RNA and whether the threat is against a high-priority target, such as an e-commerce server. The response to any given security event is predicated upon this automated, real-time intelligent analysis and could range from no action (as in the case where the Defense Center has determined that the network or the individual asset is not vulnerable to the observed threat) to blocking the threat in real time, dynamically modifying firewall policy, and/or launching configuration management software to correct a vulnerability condition.

Comprehensive Network and User Intelligence. Our innovative network security solution incorporates RNA, which provides persistent visibility into the composition, behavior, topology and risk profile of the network and serves as a platform for automated decision-making and network security policy enforcement. RNA performs passive, or non-disruptive, network discovery. This enables network behavior analysis (NBA) and real-time compositional cataloging of network assets, including their configuration, thereby significantly increasing the network intelligence available to IT and security administrators. RNA also provides the foundation for Sourcefire s innovative new Adaptive IPS strategy, which maximizes efficiency and effectiveness of the IPS by ensuring Snort rules are consistently enabled to protect actual network assets present on the protected network. With our RUA offering, Sourcefire is the first network security provider to incorporate user identity as a part of a comprehensive IPS solution. By pairing usernames with host IP addresses, Sourcefire customers can evaluate and mitigate security and compliance events in less time than it takes with an IP address alone.

The Open Source Community. The open source Snort user community, with over 170,000 registered users and over 3 million downloads to date, has enabled us to establish a strong market footprint. We believe that a majority of the Fortune 100 companies and all of the top 30 U.S. government agencies use Snort technology to monitor network traffic and that Snort is the most widely deployed intrusion prevention technology worldwide. With more than one million unique IP addresses downloading signature updates daily, ClamAV is a leading tool in the anti-malware market. We believe that the combined user communities of both Snort and ClamAV provide us with significant benefits, including a broad threat awareness network, significant research and development leverage, and a large pool of security experts that are skilled in the use of our technologies. These communities enable us to more cost-effectively test new algorithms and concepts on a vast number of diverse networks and significantly expedite the process of product innovation. We believe that the broad acceptance of Snort and ClamAV makes us one of the most trusted sources of network security solutions.

Leading-Edge Performance. Our solutions are built to maintain high performance across the network while also providing high levels of network security. Specifically, our solutions have the ability to process up to 10 gigabits of traffic with latency as low as 100 microseconds. Our IPS technology incorporates advanced traffic processing functionality, including packet acquisition, protocol normalization and target-based traffic inspection, which yields increased inspection precision and efficiency and enables more granular inspection of network traffic. The Defense Center supports event loads as high as 1,300 events per second, which we believe meets or exceeds the requirements of the most demanding enterprise customers.

Significant Security Expertise. Our senior management team has extensive network security industry experience gained from past service in leading enterprises and government organizations, including Symantec, McAfee, the Department of Defense and the National Security Agency. Our founder and CTO, Martin Roesch, invented Snort and the core RNA technology and is widely regarded as a network security visionary. In addition, our senior management team averages 16 years of experience in the networking and security industries. Our employees have authored all major components of the Snort source code and maintain the Snort project. Our Vulnerability Research Team, or VRT, is comprised of highly experienced security experts who research new vulnerabilities and create innovative methods for preventing attempts to exploit them. Tomasz Kojm, ClamAV founder, and the core ClamAV team bring valuable experience to Sourcefire in defending against viruses, trojans, spyware and other forms of malware. By combining the strengths of our Sourcefire, Snort and ClamAV development teams with the breadth of the open source community, we believe our domain knowledge places us at the leading edge of the network security industry.

Broad Industry Recognition. We have received numerous industry awards and certifications including recognition as a leader in the network IPS market, supporting our position as one of a select few companies that best combines completeness of vision with ability to execute. Sourcefire is currently the only major IPS provider to hold Network Intrusion Prevention certification from ICSA Labs, and RNA is one of only five network security products to receive the NSS Gold award, which is awarded by The NSS Group only to those products that are distinguished in terms of advanced or unique features, and which offer outstanding value. In addition, our technology has achieved Common Criteria Evaluation Assurance Level 2, or EAL2, which is an international evaluation standard for information technology security products sanctioned by, among others, the International Standards Organization, the National Security Agency and the National Institute for Standards and Technology.

Our Growth Strategy

We intend to become the preeminent provider of open source and commercial network security solutions on a global basis. The key elements of our growth strategy include:

Continue to Develop Innovative Network Security Technology. We intend to maintain and enhance our technological leadership position in network security. We will continue to invest significantly in internal development and product enhancements and to hire additional experienced network security professionals to broaden our proprietary knowledge base. We believe our platform is capable of expanding into new markets such as unified threat management, security management, network behavior analysis and compliance and network management and, over time, we expect to penetrate these markets with innovative products and technologies.

Grow Our Customer Base. We have an opportunity to grow our customer base as our products become more widely adopted. With over 3 million downloads of Snort and over 170,000 registered users, we believe Snort is the most ubiquitous network intrusion detection and prevention technology and represents a significant customer conversion and up-sell opportunity for Sourcefire. We seek to monetize the Snort installed base by targeting enterprises that implement Snort but have not yet purchased any of the components of our Sourcefire 3D system. Through December 31, 2007, over 1,700 customers have purchased our products and services. Further, Sourcefire seeks to build upon its recent investment in ClamAV by affording ClamAV users with new-found improvements in support, manageability, scalability and performance. We will continue to target enterprises and government agencies that require advanced security technology and high levels of network availability and performance in sectors including finance, technology, healthcare, manufacturing and defense. Furthermore, we may create new customer conversion and sales opportunities by releasing select future product features and enhancements under an open source form of license, similar to the sales opportunity we created for our current 3D system products by releasing Snort under an open form of license.

Further Penetrate Our Existing Customer Base. We believe our strong customer relationships provide us the opportunity to sell both additional quantities of existing products and new products. We intend to sell additional products to existing customers and expand our footprint in the networks of our customers to include branch offices, remote locations and data centers. In addition, we believe we have a significant opportunity to up-sell our higher margin RNA and RUA products to existing customers because of the significant incremental benefit that increased network intelligence can bring to their security systems.

Expand Our OEM Alliances and Distribution Relationships. We believe we have a significant opportunity to drive revenue growth through our OEM and distribution relationships. We currently have OEM relationships in place with Nokia and Nortel, and we have a partnership with Crossbeam in which our software is preinstalled on their hardware. In addition, we seek to expand our strategic reseller arrangements and increasingly use this channel to generate additional inbound customer prospects. For example, we have reseller agreements with True North Solutions, which has been acquired by American Systems Corporation, and Pentura Limited, a UK information technology security company, through which we expect to derive additional revenue growth in the future. We also intend to utilize our relationships with managed security service providers such as Symantec, BT Counterpane, SecureWorks, VeriSign and Verizon, to derive incremental revenue. In 2007, we generated approximately 11% of our revenue from governmental organizations and, in the future, we believe we will generate an increasing amount of revenue from government suppliers such as Lockheed Martin, Northrop Grumman and Immix Technology, who resell our products to government agencies.

Strengthen Our International Presence. We believe the network security needs of many enterprises located outside of North America are not being adequately served and therefore represent a significant potential market opportunity. In 2007, we generated approximately 25% of our revenue from international customers, up from 19% in 2006. We have distribution agreements with several resellers having significant foreign presence, through which we now offer the Sourcefire 3D security solution. Beyond these growing reseller relationships, we are also investing in the capacity of our international sales and channel personnel who will provide expanded levels of support to regions throughout Europe, Latin America, and the Asia Pacific.

Selectively Pursue Acquisitions of Complementary Businesses and Technologies. To accelerate our expected growth, enhance the capabilities of our existing products and broaden our product and service offerings, we intend to selectively pursue acquisitions of businesses, technologies and products that would complement our existing operations. We continually seek to enhance and expand the breadth of our products and services and in the future we may pursue acquisitions that will enable us to better satisfy our customers rigorous and evolving network security needs.

Awards and Certifications

We received numerous industry awards and certifications since January 1, 2007, including:

> *Gartner Magic Quadrant.* In January 2007 and again in February 2008, Sourcefire announced it was recognized by Gartner, Inc. as being a Leader in the Magic Quadrant for Network Intrusion Prevention System Appliances report.

ICSA Certification. Our 3D3800 Sensor achieved Network Intrusion Prevention certification from ICSA Labs. Sourcefire is currently the only major IPS vendor to hold this certification.

IT Executive of the Year. Sourcefire founder and CTO, Martin Roesch, was named Commercial IT Executive of the Year by the Tech Council of Maryland.

Bossie Awards. InfoWorld named Snort and ClamAV as Bossie (Best in Open Source Security) winners, recognizing Sourcefire s open source leadership.

SC Awards Finalist. Sourcefire was named a finalist in four categories in the 2007 SC Awards.

Customers

We provide products and services to a variety of end users worldwide. Our customers represent a broad spectrum of organizations within diverse sectors, including some of the world s largest financial institutions, defense contractors, health care providers, IT companies, telecommunication companies and retailers, as well as U.S. and other national, state and local government agencies. Through December 31, 2007, over 1,700 customers have purchased our products and services. We view our primary customers as enterprises generally having annual revenue exceeding $500 million, though we are increasingly pursuing the sale of products and services to the mid-tier market, targeting organizations with annual revenue ranging from $250-$500 million.

In 2007, 2006 and 2005, no single customer accounted for over 10% of our revenues.

Sales and Marketing

We market and sell our appliances, software and services directly to our customers through our direct sales organization and indirectly through our resellers, distributors and original equipment manufacturers (OEMs).

Sales. As of December 31, 2007, our sales organization was comprised of approximately 89 full-time individuals organized into two geographic regions: North America and International. The North America sales force was divided into three groups: East, West and Federal. We maintain sales offices in Columbia, Maryland; Vienna, Virginia; Livonia, Michigan; Wokingham, United Kingdom; Tokyo, Japan; Singapore; Courbevoie Cedex, France; Hoofddorp, The Netherlands and Espoo, Finland. Our sales personnel are responsible for market development, including managing our relationships with resellers and distributors, assisting them in winning and supporting key customer accounts and acting as liaisons between the end customers and our marketing and product development organizations. We are also investing in the capacity of our international sales and channel personnel who will provide expanded levels of support to regions throughout Europe, Latin America, and the Asia/Pacific region.

Each sales organization is supported by experienced security engineers who are responsible for providing pre-sales technical support and technical training for the sales team and for our resellers and distributors. All of our sales personnel are responsible for lead follow-up and account management. Our sales personnel have quota requirements and are compensated with a combination of base salary and earned commissions.

Our indirect sales channel, comprised primarily of resellers and distributors, is supported by our sales force, including dedicated channel managers, with substantial experience in selling network security products to, and through, resellers. We maintain a broad network of value-added resellers throughout the United States and Canada, and distributors in Europe, Latin America and Asia/Pacific. Our arrangements with our resellers are non-exclusive, generally cover all of our products and services, and provide for appropriate discounts based on a variety of factors, including their transaction volume. These agreements are generally terminable at will by either party by providing the other party at least 90 days written notice. Our arrangements with distributors also are non-exclusive, are generally territory-specific, and provide discounts generally based upon the annual volume of their orders. We also provide our resellers and distributors with marketing assistance, technical training, and support.

Strategic Relationships. We have established commercial relationships with networking and security companies to provide alternative distribution channels for our products. Sourcefire has OEM relationships with Nokia and Nortel, and a meet-in-the-middle channel relationship with Crossbeam.

Marketing. Our marketing activity consists primarily of product marketing, product management and sales support programs. Marketing also includes advertising, our corporate website, trade shows, direct marketing and public relations. Our marketing program is designed to build the Sourcefire, Snort and ClamAV brands, increase customer awareness, generate leads and communicate our product advantages. We also use our marketing program to support the sale of our products through new channels and to new markets.

Research and Development

Our research and development efforts are focused both on improving and enhancing our existing network security products and on developing new features and functionality. We communicate with our customers and the open source community when considering product improvements and enhancements, and we regularly release new versions of our products incorporating these improvements and enhancements.

Vulnerability Research Team. Our Vulnerability Research Team is a group of leading edge network security experts working to proactively discover, assess and respond to the latest trends in network threats and security vulnerabilities. By gathering and analyzing this information, our Vulnerability Research Team creates and updates Snort rules, ClamAV signatures, and security tools that are designed to identify, characterize and defeat attacks. This team comprises full-time employees and operates from our corporate headquarters in Columbia, Maryland. Our Vulnerability Research Team participates in extensive collaboration with hundreds of network security professionals in the open source Snort community to learn of new vulnerabilities and exploits. The Vulnerability Research Team also coordinates and shares information with other security authorities such as The SANS Institute, CERT-CC (Computer Emergency Response Team), iDefense (Verisign), SecurityFocus (Bugtraq; Symantec) and Common Vulnerabilities and Exposures (Mitre). Because of the knowledge and experience of our personnel comprising the Vulnerability Research Team, as well as its extensive coordination with the open source community, we believe that we have access to one of the largest and most sophisticated groups of IT security experts researching vulnerability and threats on a real-time basis.

Our research and development expense was $11.9 million, $8.6 million and $6.8 million for the years ended December 31, 2007, 2006 and 2005, respectively.

Manufacturing and Suppliers

We rely primarily on contract equipment manufacturers to assemble, integrate and test our appliances and to ship those appliances to our customers. We typically hold little inventory, relying instead on a just-in-time manufacturing philosophy. We rely on three primary integrators. We have contracted with Patriot Technologies, Inc. and Intelligent Decisions Inc., or IDI, to assemble, integrate and test all our product offerings operating on an Intel platform. Our agreement with Patriot expires on December 12, 2008, and will automatically renew for successive one-year periods unless either we or Patriot notify the other of an intent not to renew at least 90 days prior to expiration. Our agreement with IDI expires on January 31, 2009 and will automatically renew for successive one-year periods unless either party notifies the other party of its intent not to renew at least 30 days prior to the end of the term. Finally, we have contracted with Bivio Networks, Inc. to manufacture select high performance models of our appliances. Bivio is our sole supplier of these high performance models, such as our 3D3800, 3D5800 and 3D9800, which are the highest priced 3D Sensors that we offer. Our agreement with Bivio expires on February 10, 2010. All of these agreements are non-exclusive. We would be faced with the burden, cost and delay of having to qualify and contract with a new supplier if any of these agreements terminate or expire for any reason.

Intellectual Property

To protect our intellectual property, both domestically and abroad, we rely primarily on patent, trademark, copyright and trade secret laws. We hold three issued patents and have 33 patent applications pending for examination in the U.S. and foreign jurisdictions. The claims for which we have sought patent protection relate to methods and systems we have developed for intrusion detection and prevention used in our RNA, IPS and Defense Center products. In addition, we utilize contractual provisions, such as non-disclosure and non-compete agreements with our employees and consultants, as well as confidentiality procedures to strengthen our protection.

Despite our efforts to protect our intellectual property, unauthorized parties may attempt to copy aspects of our products or obtain and use information that we regard as proprietary. While we cannot determine the extent to which piracy of our software products occurs, we expect software piracy to be a persistent problem. In addition, the laws of some foreign countries do not protect our proprietary rights to as great an extent as do the laws of the United States, and many foreign countries do not enforce these laws as diligently as U.S. government agencies and private parties.

Seasonality

Our business is subject to seasonal fluctuations. For a discussion of seasonality affecting our business, see Management s Discussion and Analysis of Financial Condition and Results of Operations Results of Operations Seasonality.

Competition

The market for network security monitoring, detection, prevention and response solutions is intensely competitive and we expect strong competition to continue in the future. Our chief competitors generally fall within the following categories:

large companies, including Cisco Systems, Inc., IBM Corporation, Juniper Networks, Inc., 3Com Corporation, Check Point Software Technologies, Ltd. and McAfee, Inc., that sell competitive products and offerings, as well as other large software companies that have the technical capability and resources to develop competitive products;

software or hardware network infrastructure companies, including Cisco Systems, Inc., 3Com Corporation and Juniper Networks, Inc., that could integrate features that are similar to our products into their own products;

smaller software companies offering relatively limited applications for network and Internet security monitoring, detection, prevention or response; and

small and large companies offering point solutions that compete with components of our product offerings.

Mergers or consolidations among these competitors, or acquisitions of our competitors by large companies, present competitive challenges to our business. For example, during the past several years IBM Corporation, Cisco Systems, Inc., McAfee, Inc., 3Com Corporation and Juniper Networks, Inc. have acquired smaller companies that have intrusion detection and prevention technologies. These acquisitions will potentially make these combined entities more formidable competitors to us if such products and offerings are effectively integrated. Large companies may have advantages over us because of their longer operating histories, greater brand name recognition, larger customer bases or greater financial, technical and marketing resources. As a result, they may be able to adapt more quickly to new or emerging technologies and changes in customer requirements. They also have greater resources to devote to the promotion and sale of their products. In addition, these companies have reduced and could continue to reduce, the price of their security monitoring, detection, prevention and response products and managed security services, which intensifies pricing pressures within our market.

Several companies currently sell security software products (such as encryption, firewall, operating system security and virus detection software) that our customers and potential customers have broadly adopted. Some of these companies sell products that perform the same functions as some of our products. In addition, the vendors of operating system software or networking hardware may enhance their products to include functions similar to those that our products currently provide.

We believe that the principal competitive factors affecting the market for information security solutions include security effectiveness, manageability, technical features, performance, ease of use, price, scope of product offerings, professional services capabilities, distribution relationships and customer service and support. We believe that our solutions generally compete favorably with respect to such factors.

Employees

As of December 31, 2007, we had 240 employees, of whom 72 were engaged in product research and development, 103 were engaged in sales and marketing, 15 were engaged in customer service and support, 10 were engaged in professional services and 40 were engaged in administrative functions. Our current employees are not represented by a labor union and are not the subject of a collective bargaining agreement. We believe that we have good relations with our employees.

Corporate Information

Sourcefire, Inc. was organized in Delaware in January 2001. We completed our initial public offering in March 2007. Our executive offices are located at 9770 Patuxent Woods Drive, Columbia, Maryland 21046, and our main telephone number is (410) 290-1616.

Available Information

Our internet address is www.sourcefire.com. We provide free of charge on the Investor Relations page of our web site access to our annual report on Form 10-K, quarterly reports on Form 10-Q, current reports on Form 8-K and amendments to those reports as soon as reasonably practicable after they are electronically filed with or furnished to the Securities and Exchange Commission (SEC). Information appearing on our website is not incorporated by reference in and is not a part of this report.

Item 1A. *RISK FACTORS*

Set forth below and elsewhere in this Annual Report on Form 10-K, and in other documents we file with the Securities and Exchange Commission, are risks and uncertainties that could cause actual results to differ materially from the results contemplated by the forward-looking statements contained in this Annual Report on Form 10-K. Because of the following factors, as well as other variables affecting our operating results, past financial performance should not be considered as a reliable indicator of future performance, and investors should not use historical trends to anticipate results or trends in future periods.

We have had operating losses since our inception, we expect operating expenses to increase in the foreseeable future and we may never reach or maintain profitability.

We have incurred operating losses each year since our inception in 2001. Our net loss was approximately $932,000 for the year ended December 31, 2006 and $5.6 million for the year ended December 31, 2007. Our accumulated deficit as of December 31, 2007 is approximately $44.5 million. Becoming profitable will depend in large part on our ability to generate and sustain increased revenue levels in future periods. Although our revenue has generally been increasing, there can be no assurances that we will become profitable in the near future or at any other time. We may never achieve profitability and, even if we do, we may not be able to maintain or increase our level of profitability. We expect that our operating expenses will continue to increase in the foreseeable future as we seek to expand our customer base, increase our sales and marketing efforts, continue to invest in research and development of our technologies and product enhancements and incur significant costs associated with being a public company. These efforts may be more costly than we expect and we may not be able to increase our revenue enough to offset our higher operating expenses. In addition, if our new products and product enhancements fail to achieve adequate market acceptance, our revenue will suffer. If we cannot increase our revenue at a greater rate than our expenses, we will not become or remain profitable.

We face intense competition in our market, especially from larger, better-known companies, and we may lack sufficient financial or other resources to maintain or improve our competitive position.

The market for network security monitoring, detection, prevention and response solutions is intensely competitive, and we expect competition to increase in the future. We may not compete successfully against our current or potential competitors, especially those with significantly greater financial resources or brand name recognition. Our chief competitors include large software companies, software or hardware network infrastructure companies, smaller software companies offering relatively limited applications for network and Internet security monitoring, detection, prevention or response and small and large companies offering point solutions that compete with components of our product offerings.

Mergers or consolidations among these competitors, or acquisitions of our competitors by large companies, present heightened competitive challenges to our business. For example, Cisco Systems, Inc., McAfee, Inc., 3Com Corporation, Juniper Networks, Inc. and IBM have acquired, during the past several years, smaller companies that have intrusion detection or prevention technologies. These acquisitions may make these combined entities more formidable competitors to us if such products and offerings are effectively integrated. Large companies may have advantages over us because of their longer operating histories, greater brand name recognition, larger customer bases or greater financial, technical and marketing resources. As a result, they may be able to adapt more quickly to new or emerging technologies and changes in customer requirements. They also have greater resources to devote to the promotion and sale of their products than we have. In addition, these companies have reduced and could continue to reduce, the price of their security monitoring, detection, prevention and response products and managed security services, which intensifies pricing pressures within our market.

Several companies currently sell software products (such as encryption, firewall, operating system security and virus detection software) that our customers and potential customers have broadly adopted. Some of these companies sell products that perform functions comparable to some of our products. In addition, the vendors of operating system software or networking hardware may enhance their products to include functions similar to those that our products currently provide. The widespread inclusion of comparable features comparable to our software in operating system software or networking hardware could render our products less competitive or obsolete, particularly if such features are of a high quality. Even if security functions integrated into operating system software or networking hardware are more limited than those of our products, a significant number of customers may accept more limited functionality to avoid purchasing additional products such as ours.

One of the characteristics of open source software is that anyone can offer new software products for free under an open source licensing model in order to gain rapid and widespread market acceptance. Such competition can develop without the degree of overhead and lead time required by traditional technology companies. It is possible for new competitors with greater resources than ours to develop their own open source security solutions, potentially reducing the demand for our solutions. We may not be able to compete successfully against current and future competitors. Competitive pressure and/or the availability of open source software may result in price reductions, reduced revenue, reduced operating margins and loss of market share, any one of which could seriously harm our business.

New competitors could emerge or our customers or distributors could internally develop alternatives to our products, and either such development could impair our sales.

We may face competition from emerging companies as well as established companies who have not previously entered the market for network security products. Established companies may not only develop their own network intrusion detection and prevention products, but they may also acquire or establish product integration, distribution or other cooperative relationships with our current competitors. Moreover, our large corporate customers and potential customers could develop network security software internally, which would reduce our potential revenue. New competitors or alliances among competitors may emerge and rapidly acquire significant market share due to factors such as greater brand name recognition, a larger installed customer base and significantly greater financial, technical, marketing and other resources and experience.

Our quarterly operating results are likely to vary significantly and be unpredictable, in part because of the purchasing and budget practices of our customers, which could cause the trading price of our stock to decline.

Our operating results have historically varied significantly from period to period, and we expect that they will continue to do so as a result of a number of factors, most of which are outside of our control, including:

the budgeting cycles, internal approval requirements and funding available to our existing and prospective customers for the purchase of network security products;

the timing, size and contract terms of orders received, which have historically been highest in the fourth quarter (representing more than one-third of our total revenue in recent years), but may fluctuate seasonally in different ways;

the level of perceived threats to network security, which may fluctuate from period to period;

the level of demand for products sold by original equipment manufacturers, or OEMs, resellers and distributors that incorporate and resell our technologies;

the market acceptance of open-source software solutions;

the announcement or introduction of new product offerings by us or our competitors, and the levels of anticipation and market acceptance of those products;

price competition;

general economic conditions, both domestically and in our foreign markets;

the product mix of our sales; and

the timing of revenue recognition for our sales.

In particular, the network security technology procurement practices of many of our customers have had a measurable influence on the historical variability of our operating performance. Our prospective customers usually exercise great care and invest substantial time in their network security technology purchasing decisions. As a result, our sales cycles are long, generally between six and twelve months and often longer, which further impacts the variability of our results. Additionally, many of our customers have historically finalized purchase decisions in the last weeks or days of a quarter. A delay in even one large order beyond the end of a particular quarter can substantially diminish our anticipated revenue for that quarter. In addition, many of our expenses must be incurred before we generate revenue. As a result, the negative impact on our operating results would increase if our revenue fails to meet expectations in any period.

The cumulative effect of these factors will likely result in larger fluctuations and unpredictability in our quarterly operating results than in the operating results of many other software and technology companies. This variability and unpredictability could result in our failing to meet the revenue or operating results expectations of securities industry analysts or investors for a particular period. If we fail to meet or exceed such expectations for these or any other reasons, the market price of our shares could fall substantially, and we could face costly securities class action suits as a result. Therefore, you should not rely on our operating results in any quarter as being indicative of our operating results for any future period, nor should you rely on other expectations, predictions or projections of our future revenue or other aspects of our results of operations.

Economic, market and political conditions may adversely affect our revenue growth and our efforts to achieve profitability.

Our business is influenced by a range of factors that are beyond our control. These include:

general economic and business conditions;

the overall demand for network security products and services; and

constraints on budgets and changes in spending priorities of corporations and government agencies.

A general weakening of the economy in the United States or of the global economy, or a curtailment in corporate spending due to factors that affect one or more of the industries to which we sell our products and services, could delay and decrease customer purchases, which could adversely affect our revenue growth and results of operations. For example, the decline in operating performance of financial institutions associated with the problems in the subprime mortgage industry could cause our current or potential financial institution customers to delay or forego purchases of our products and services. Our customers include, but are not limited to, financial institutions, defense contractors, health care providers, IT companies, telecommunications companies and retailers. Similarly, a reduction in the budgets or spending priorities of government agencies could adversely affect our revenue growth and results of operations.

The market for network security products is rapidly evolving, and the complex technology incorporated in our products makes them difficult to develop. If we do not accurately predict, prepare for and respond promptly to technological and market developments and changing customer needs, our competitive position and prospects will be harmed.

The market for network security products is relatively new and is expected to continue to evolve rapidly. Moreover, many customers operate in markets characterized by rapidly changing technologies and business plans, which require them to add numerous network access points and adapt increasingly complex enterprise networks, incorporating a variety of hardware, software applications, operating systems and networking protocols. In addition, computer hackers and others who try to attack networks employ increasingly sophisticated new techniques to gain access to and attack systems and networks. Customers look to our products to continue to protect their networks against these threats in this increasingly complex environment without sacrificing network efficiency or causing significant network downtime. The software in our products is especially complex because it needs to effectively identify and respond to new and increasingly sophisticated methods of attack, without impeding the high network performance demanded by our customers. Although the market expects speedy introduction of software to respond to new threats, the development of these products is difficult and the timetable for commercial release of new products is uncertain. Therefore, we may in the future experience delays in the introduction of new products or new versions, modifications or enhancements of existing products. If we do not quickly respond to the rapidly changing and rigorous needs of our customers by developing and introducing on a timely basis new and effective products, upgrades and services that can respond adequately to new security threats, our competitive position and business prospects will be harmed.

If our new products and product enhancements do not achieve sufficient market acceptance, our results of operations and competitive position will suffer.

We spend substantial amounts of time and money to research and develop new products and enhanced versions of Snort, the Defense Center and our 3D Sensor and RNA products to incorporate additional features, improved functionality or other enhancements in order to meet our customers rapidly evolving demands for network security in our highly competitive industry. When we develop a new product or an advanced version of an existing product, we typically expend significant money and effort upfront to market, promote and sell the new offering. Therefore, when we develop and introduce new or enhanced products, they must achieve high levels of market acceptance in order to justify the amount of our investment in developing and bringing the products to market.

Our new products or enhancements could fail to attain sufficient market acceptance for many reasons, including:

- delays in introducing new, enhanced or modified products;
- defects, errors or failures in any of our products;
- inability to operate effectively with the networks of our prospective customers;
- inability to protect against new types of attacks or techniques used by hackers;
- negative publicity about the performance or effectiveness of our intrusion prevention or other network security products;
- reluctance of customers to purchase products based on open source software; and
- disruptions or delays in the availability and delivery of our products, which problems are more likely due to our just-in-time manufacturing and inventory practices.

If our new products or enhancements do not achieve adequate acceptance in the market, our competitive position will be impaired, our revenue will be diminished and the effect on our operating results may be particularly acute because of the significant research, development, marketing, sales and other expenses we incurred in connection with the new product.

If existing customers do not make subsequent purchases from us or if our relationships with our largest customers are impaired, our revenue could decline.

In 2005, 2006 and 2007, existing customers that purchased additional products and services from us, whether for new locations or additional technology to protect existing networks and locations, generated a majority of our total revenue for each respective period. Part of our growth strategy is to sell additional products to our existing customers and, in particular, to sell our RNA products to customers that previously bought our Intrusion Sensor products. We may not be effective in executing this or any other aspect of our growth strategy. Our revenue could decline if our current customers do not continue to purchase additional products from us. In addition, as we deploy new versions of our existing Snort, 3D Sensor and RNA products or introduce new products, our current customers may not require the functionality of these products and may not purchase them.

We also depend on our installed customer base for future service revenue from annual maintenance fees. Our maintenance and support agreements typically have durations of one year. No single customer contributed greater than 10% of our recurring maintenance and support revenues in 2005, 2006 or 2007. If customers choose not to continue their maintenance service, our revenue may decline.

If we cannot attract sufficient government agency customers, our revenue and competitive position will suffer.

Contracts with the U.S. federal and state and other national and state government agencies accounted for 11% of our total revenue for both of the years ended December 31, 2006 and December 31, 2007. We lost many government agency customers when a foreign company tried unsuccessfully to acquire us in late 2005 and early 2006. Since then, we have been attempting to regain government customers, which subjects us to a number of risks, including:

Procurement. Contracting with public sector customers is highly competitive and can be expensive and time-consuming, often requiring that we incur significant upfront time and expense without any assurance that we will win a contract;

Budgetary Constraints and Cycles. Demand and payment for our products and services are impacted by public sector budgetary cycles and funding availability, with funding reductions or delays adversely impacting public sector demand for our products, including delays caused by continuing resolutions or other temporary funding arrangements;

Modification or Cancellation of Contracts. Public sector customers often have contractual or other legal rights to terminate current contracts for convenience or due to a default. If a contract is cancelled for convenience, which can occur if the customer s product needs change, we may only be able to collect for products and services delivered prior to termination. If a contract is cancelled because of default, we may only be able to collect for products and alternative products and services delivered to the customer;

Governmental Audits. National governments and state and local agencies routinely investigate and audit government contractors administrative processes. They may audit our performance and pricing and review our compliance with applicable rules and regulations. If they find that we improperly allocated costs, they may require us to refund those costs or may refuse to pay us for outstanding balances related to the improper allocation. An unfavorable audit could result in a reduction of revenue, and may result in civil or criminal liability if the audit uncovers improper or illegal activities; and

Replacing Existing Products. Many government agencies already have installed network security products of our competitors. It can be very difficult to convince government agencies or other prospective customers to replace their existing network security solutions with our products, even if we can demonstrate the superiority of our products.

We are subject to risks of operating internationally that could impair our ability to grow our revenue abroad.

We market and sell our software in North America, South America, Europe, Asia and Australia, and we plan to establish additional sales presence in these and other parts of the world. Therefore, we are subject to risks associated with having worldwide operations. Sales to customers located outside of the United States accounted for 19% of our total revenue for the year ended December 31, 2006 and 25% for the year ended December 31, 2007. The expansion of our existing operations and entry into additional worldwide markets will require significant management attention and financial resources. We are also subject to a number of risks customary for international operations, including:

economic or political instability in foreign markets;

greater difficulty in accounts receivable collection and longer collection periods;

unexpected changes in regulatory requirements;

difficulties and costs of staffing and managing foreign operations;

import and export controls;

the uncertainty of protection for intellectual property rights in some countries;

costs of compliance with foreign laws and laws applicable to companies doing business in foreign jurisdictions;

management communication and integration problems resulting from cultural differences and geographic dispersion;

multiple and possibly overlapping tax structures; and

foreign currency exchange rate fluctuations.

To date, a substantial portion of our sales have been denominated in U.S. dollars, and we have not used risk management techniques or hedged the risks associated with fluctuations in foreign currency exchange rates. In the future, if we do not engage in hedging transactions, our results of operations will be subject to losses from fluctuations in foreign currency exchange rates.

In the future, we may not be able to secure financing necessary to operate and grow our business as planned.

In the future, we may need to raise additional funds to expand our sales and marketing and research and development efforts or to make acquisitions. Additional equity or debt financing may not be available on favorable terms, if at all. If adequate funds are not available on acceptable terms, we may be unable to fund the expansion of our sales and marketing and research and development efforts or take advantage of acquisition or other opportunities, which could seriously harm our business and operating results. If we issue debt, the debt holders would have rights senior to common stockholders to make claims on our assets and the terms of any debt could restrict our operations, including our ability to pay dividends on our common stock. Furthermore, if we issue additional equity securities, stockholders would experience dilution, and the new equity securities could have rights senior to those of our common stock.

Our inability to acquire and integrate other businesses, products or technologies could seriously harm our competitive position.

In order to remain competitive, we intend to acquire additional businesses, products or technologies. If we identify an appropriate acquisition candidate, we may not be successful in negotiating the terms of the acquisition, financing the acquisition, or effectively integrating the acquired business, product or technology into our existing business and operations. Any acquisitions we are able to complete may not be accretive to earnings or result in the realization of any expected strategic benefits. Further, completing a potential acquisition and integrating an acquired business could significantly divert management s time and resources from the operation of our business.

If other parties claim commercial ownership rights to Snort or ClamAV, our reputation, customer relations and results of operations could be harmed.

While we created a majority of the current Snort code base and the current ClamAV code base, a portion of the current code for both Snort and ClamAV was created by the combined efforts of Sourcefire and the open source software community, and a portion was created solely by the open source community. We believe that the portions of the Snort code base and the ClamAV base code created by anyone other than by us are required to be licensed by us pursuant to the GNU General Public License, or GPL, which is how we currently license Snort and ClamAV. There is a risk, however, that a third party could claim some ownership rights in Snort or ClamAV, attempt to prevent us from commercially licensing Snort or ClamAV in the future (rather than pursuant to the GPL as currently licensed) or claim a right to licensing royalties. Any such claim, regardless of its merit or outcome, could be costly to defend, harm our reputation and customer relations or result in our having to pay substantial compensation to the party claiming ownership.

Our products contain third party open source software, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products.

Our products are distributed with software programs licensed to us by third party authors under open source licenses, which may include the GPL, the GNU Lesser Public License, or LGPL, the BSD License and the Apache License. These open source software programs include, without limitation, Snort®, ClamAVtm, Linux, Apache, Openssl, Etheral, IPTables, Tcpdump and Tripwire. These third party open source programs are typically licensed to us for a minimal fee or no fee at all, and the underlying license agreements generally require us to make available to the open source user community the source code for such programs, as well as the source code for any modifications or derivative works we create based on these third party open source software programs. With the exception of Snort and ClamAV, we have not created any modifications or derivative works to any other open source software programs referenced above. We regularly release updates and upgrades to the Snort and ClamAV software programs under the terms and conditions of the GNU GPL version 2.

Included with our software and/or appliances are copies of the relevant source code and licenses for the open source programs. Alternatively, we include instructions to users on how to obtain copies of the relevant open source code and licenses. Additionally, if we combine our proprietary software with third party open source software in a certain manner, we could, under the terms of certain of these open source license agreements, be required to release the source code of our proprietary software. This could also allow our competitors to create similar products, which would result in a loss of our product sales. We do not provide end users with a copy of the source code to our proprietary software because we believe that the manner in which our proprietary software is aligned with the relevant open source programs does not create a modification or derivative work of that open source program requiring the distribution of our proprietary source code. Our ability to commercialize our products by incorporating third party open source software may be restricted because, among other reasons:

the terms of open source license agreements may be unclear and subject to varying interpretations, which could result in unforeseen obligations regarding our proprietary products;

it may be difficult to determine the developers of open source software and whether such licensed software infringes another party s intellectual property rights;

competitors will have greater access to information by obtaining these open source products, which may help them develop competitive products; and

open source software potentially increases customer support costs because licensees can modify the software and potentially introduce errors.

We could be prevented from selling or developing our products if the GNU General Public License and similar licenses under which our products are developed and licensed are not enforceable or are modified so as to become incompatible with other open source licenses.

A number of our products and services have been developed and licensed under the GNU General Public License and similar open source licenses. These licenses state that any program licensed under them may be liberally copied, modified and distributed. It is possible that a court would hold these licenses to be unenforceable in that or other litigation or that someone could assert a claim for proprietary rights in a program developed and distributed under them. Any ruling by a court that these licenses are not enforceable, or that open source components of our product offerings may not be liberally copied, modified or distributed, may have the effect of preventing us from distributing or developing all or a portion of our products. In addition, licensors of open source software employed in our offerings may, from time to time, modify the terms of their license agreements in such a manner that those license terms may no longer be compatible with other open source licenses in our offerings or our end user license agreement, and thus could, among other consequences, prevent us from continuing to distribute the software code subject to the modified license.

The software program Linux is included in our products and is licensed under the GPL. The GPL is the subject of litigation in the case of The SCO Group, Inc. v. International Business Machines Corp., pending in the United States District Court for the District of Utah. It is possible that the court could rule that the GPL is not enforceable in such litigation. Any ruling by the court that the GPL is not enforceable could have the effect of limiting or preventing us from using Linux as currently implemented.

Efforts to assert intellectual property ownership rights in our products could impact our standing in the open source community, which could limit our product innovation capabilities.

If we were to undertake actions to protect and maintain ownership and control over our proprietary intellectual property, including patents, copyrights, trademark rights and trade secrets, our standing in the open source community could be diminished which could result in a limitation on our ability to continue to rely on this community as a resource to identify and defend against new viruses, threats and techniques to attack secure networks, explore new ideas and concepts and further our research and development efforts.

Our proprietary rights may be difficult to enforce, which could enable others to copy or use aspects of our products without compensating us.

We rely primarily on copyright, trademark, patent and trade secret laws, confidentiality procedures and contractual provisions to protect our proprietary rights. As of the date hereof, we have three patents issued and 33 applications pending for examination in the U.S. and foreign jurisdictions. We also hold numerous registered United States and foreign trademarks and have a number of trademark applications pending in the United States and in foreign jurisdictions. Valid patents may not be issued from pending applications, and the claims allowed on any patents may not be sufficiently broad to protect our technology or products. Any issued patents may be challenged, invalidated or circumvented, and any rights granted under these patents may not actually provide adequate protection or competitive advantages to us. Despite our efforts to protect our proprietary rights, unauthorized parties may attempt to copy aspects of our products or to obtain and use information that we regard as proprietary. Policing unauthorized use of our technologies or products is difficult. Our products incorporate open source Snort and ClamAV software, which is readily available to the public. To the extent that our proprietary software is included by others in what are purported to be open source products, it may be difficult and expensive to enforce our rights in such software. In addition, the laws of some foreign countries do not protect our proprietary rights to as great an extent as do the laws of the United States, and many foreign countries do not enforce these laws as diligently as U.S. government agencies and private parties. It is possible that we may have to resort to litigation to enforce and protect our copyrights, trademarks, patents and trade secrets, which litigation could be costly and a diversion of management resources. If we are unable to protect our proprietary rights to the totality of the features in our software and products (including aspects of our software and products protected other than by patent rights), we may find ourselves at a competitive disadvantage to others who need not incur the additional expense, time and effort required to create products similar to ours.

In limited instances we have agreed to place, and in the future may place, source code for our software in escrow, other than the Snort and ClamAV source code, which are publicly available. In most cases, the source code may be made available to certain of our customers and OEM partners in the event that we file for bankruptcy or materially fail to support our products. Release of our source code may increase the likelihood of misappropriation or other misuse of our software. We have agreed to source code escrow arrangements in the past only rarely and usually only in connection with prospective customers considering a significant purchase of our products and services.

Claims that our products infringe the proprietary rights of others could harm our business and cause us to incur significant costs.

Technology products such as ours, which interact with multiple components of complex networks, are increasingly subject to infringement claims as the functionality of products in different industry segments overlaps. In particular, our RNA technology is a new technology for which we have yet be issued a patent. It is possible that other companies have patents with respect to technology similar to our technology, including RNA. 10 of our 33 pending patent applications relate to our RNA technology and were filed in 2004 and 2005. If others filed patent applications before us, which contain allowable claims within the scope of our RNA technology, then we may be found to infringe on such patents, if and when they are issued. We are aware of at least one company that has filed an application for a patent that, on its face, contains claims that may be construed to be within the scope of the same broad technology area as our RNA technology. That company, NetClarity, previously filed a suit against us for misappropriation and incorporation in our products of its proprietary rights, as well as making claims that our RNA technology and 3D security solutions are covered by claims in its pending patent application. This pending patent application has not issued as a patent. On June 7, 2007, we reached a definitive agreement with NetClarity, Inc. to settle this lawsuit and on June 13, 2007, the Superior Court of Suffolk County, Massachusetts entered a Stipulation of Dismissal with prejudice.

Unless and until the U.S. Patent and Trademark Office, or PTO, issues a patent to an applicant, there can be no way to assess a potential patentee s right to exclude. Depending on the timing and substance of these patents and patent applications, our products, including our RNA technology, may be found to infringe the proprietary rights of others, and we may be subject to litigation with respect to any alleged infringement. The application of patent law to the software industry is particularly uncertain, as the PTO has only recently begun to issue software patents in large numbers, and there is a backlog of software-related patent applications pending claiming inventions whose priority dates may pre-date development of our own proprietary software. Additionally, in our customer contracts we typically agree to indemnify our customers if they incur losses resulting from a third party claim that their use of our products infringes upon the intellectual property rights of a third party. Any potential intellectual property claims against us, with or without merit, could:

be very expensive and time consuming to defend;

require us to indemnify our customers for losses resulting from such claims;

cause us to cease making, licensing or using software or products that incorporate the challenged intellectual property;

cause product shipment and installation delays;

require us to redesign our products, which may not be feasible;

divert management s attention and resources; or

require us to enter into royalty or licensing agreements in order to obtain the right to use a necessary product or component.

Royalty or licensing agreements, if required, may not be available on acceptable terms, or at all. A successful claim of infringement against us and our failure or inability to license the infringed or similar technology could prevent us from distributing our products and cause us to incur great expense and delay in developing non-infringing products.

We rely on software licensed from other parties, the loss of which could increase our costs and delay software shipments.

We utilize various types of software licensed from unaffiliated third parties. For example, we license database software from MySQL that we use in our 3D Sensors, our RNA Sensors and our Defense Centers. Our Agreement with MySQL permits us to distribute MySQL software on our products to our customers worldwide until December 31, 2010. We amended our MySQL agreement on December 29, 2006 to give us the unlimited right to distribute MySQL software in exchange for a one-time lump-sum payment. We believe that the MySQL agreement is material to our business because we have spent a significant amount of development resources to allow the MySQL software to function in our products. If we were forced to find replacement database software for our products, we would be required to expend resources to implement a replacement database in our products, and there would be no guarantee that we would be able to procure the replacement on the same or similar commercial terms.

In addition to MySQL, we rely on other open source software, such as the Linux operating system, the Apache web server and OpenSSL, a secure socket layer implementation. These open source programs are licensed to us under various open source licenses. For example, Linux is licensed under the GNU General Public License Version 2, while Apache and OpenSSL are licensed under other forms of open source license agreements. If we could no longer rely on these open source programs, the functionality of our products would be impaired, and we would be required to expend significant resources to find suitable alternatives.

Our business would be disrupted if any of the software we license from others or functional equivalents of this software were either no longer available to us, no longer offered to us on commercially reasonable terms or offered to us under different licensing terms and conditions. For example, our business could be disrupted if the widely-used Linux operating system were to be released under the new Version 3 of the GNU General Public License, as we could be required to expend significant resources to ensure that our use of Linux, as well as the manner in which our proprietary and other third party software work with Linux, complies with the new version of the GNU General Public License. Additionally, we would be required to either redesign our products to function with software available from other parties or develop these components ourselves, which would result in increased costs and could result in delays in our product shipments and the release of new product offerings. Furthermore, we might be forced to limit the features available in our current or future products. If we fail to maintain or renegotiate any of these software licenses, we could face significant delays and diversion of resources in attempting to license and integrate a functional equivalent of the software.

Defects, errors or vulnerabilities in our software products would harm our reputation and divert resources.

Because our products are complex, they may contain defects, errors or vulnerabilities that are not detected until after our commercial release and installation by our customers. We may not be able to correct any errors or defects or address vulnerabilities promptly, or at all. Any defects, errors or vulnerabilities in our products could result in:

- expenditure of significant financial and product development resources in efforts to analyze, correct, eliminate or work-around errors or defects or to address and eliminate vulnerabilities;
- loss of existing or potential customers;
- delayed or lost revenue;
- delay or failure to attain market acceptance;
- increased service, warranty, product replacement and product liability insurance costs; and
- negative publicity, which would harm our reputation.

In addition, because our products and services provide and monitor network security and may protect valuable information, we could face claims for product liability, tort or breach of warranty. Anyone who circumvents our security measures could misappropriate the confidential information or other valuable property of customers using our products, or interrupt their operations. If that happens, affected customers or others may sue us. In addition, we may face liability for breaches of our product warranties, product failures or damages caused by faulty installation of our products. Provisions in our contracts relating to warranty disclaimers and liability limitations may be deemed by a court to be unenforceable. Some courts, for example, have found contractual limitations of liability in standard computer and software contracts to be unenforceable in some circumstances. Defending a lawsuit, regardless of its merit, could be costly and divert management attention. Our business liability insurance coverage may be inadequate or future coverage may be unavailable on acceptable terms or at all.

Our networks, products and services are vulnerable to, and may be targeted by, hackers.

Like other companies, our websites, networks, information systems, products and services may be targets for sabotage, disruption or misappropriation by hackers. As a leading network security solutions company, we are a high profile target and our networks, products and services may have vulnerabilities that may be targeted by hackers. Although we believe we have sufficient controls in place to prevent disruption and misappropriation, and to respond to such situations, we expect these efforts by hackers to continue. If these efforts are successful, our operations, reputation and sales could be adversely affected.

We utilize a just-in-time contract manufacturing and inventory process, which increases our vulnerability to supply disruption.

Our ability to meet our customers   demand for certain of our products depends upon obtaining adequate hardware platforms on a timely basis, which must be integrated with our software. We purchase hardware platforms through our contract manufacturers from a limited number of suppliers on a just-in-time basis. In addition, these suppliers may extend lead times, limit the supply to our manufacturers or increase prices due to capacity constraints or other factors. Although we work closely with our manufacturers and suppliers to avoid shortages, we may encounter these problems in the future. Our results of operations would be adversely affected if we were unable to obtain adequate supplies of hardware platforms in a timely manner or if there were significant increases in the costs of hardware platforms or problems with the quality of those hardware platforms.

We depend on a single source to manufacture our enterprise class intrusion sensor product; if that sole source were to fail to satisfy our requirements, our sales revenue would decline and our reputation would be harmed.

We rely on one manufacturer, Bivio Networks, to build the hardware platform for three models of our intrusion sensor products that are used by our enterprise class customers. These enterprise class intrusion sensor products are purchased directly by customers for their internal use and are also utilized by third party managed security service providers to provide services to their customers. Revenue resulting from sales of these enterprise class intrusion sensor products accounted for approximately 4% of our product revenue in the year ended December 31, 2005, approximately 21% of our product revenue in the year ended December 31, 2006 and approximately 22% of our product revenue in the year ended December 31, 2007. The unexpected termination of our relationship with Bivio Networks would be disruptive to our business and our reputation, which could result in a material decline in our revenue as well as shipment delays and possible increased costs as we seek and implement production with an alternative manufacturer.

Our expected transition to a new chief executive officer could be disruptive to our business, and our inability to hire or retain other key personnel would also slow our growth.

On February 27, 2008, we announced that we and E. Wayne Jackson III, our Chief Executive Officer, had agreed not to renew the term of Mr. Jackson s employment contract with us, which is scheduled to expire at the close of business on May 5, 2008. Our board of directors has initiated an external search process for a new Chief Executive Officer to succeed Mr. Jackson, who will remain in his current role as Chief Executive Officer until we hire a successor.

While Mr. Jackson is fully cooperating with the search process, there can be no assurances that the transition to a new Chief Executive Officer will be smooth. Our success depends in part on having a successful Chief Executive Officer, yet we face significant competition for such an executive. We may not be able to find a suitable successor for the Chief Executive Officer position in a timely manner, and there are also no assurances that a new Chief Executive Officer would lead us in a successful manner. Any failure to implement a smooth transition to such a successor could have a material adverse effect on our business, results of operations or financial condition.

In addition to the transition of our Chief Executive Officer position, our business is also dependent on our ability to hire, retain and motivate highly qualified personnel, including other senior management, sales and technical professionals. In particular, as part of our growth strategy we intend to expand the size of our direct sales force domestically and internationally and to hire additional customer support and professional services personnel. However, competition for qualified services personnel is intense, and if we are unable to attract, train or retain the number of highly qualified sales and services personnel that our business needs, our reputation, customer satisfaction and potential revenue growth could be seriously harmed. To the extent that we hire personnel from competitors, we may also be subject to allegations that they have been improperly solicited or divulged proprietary or other confidential information.

In light of the transition arrangement with Mr. Jackson as our Chief Executive Officer, our future success will depend to a significant extent on the continued services of Martin Roesch, our founder. The loss of the services of this or other individuals could adversely affect our business and could divert other senior management time in searching for their replacements.

We depend on resellers and distributors for our sales; if they fail to perform as expected, our revenue will suffer.

Part of our business strategy involves entering into additional agreements with resellers and distributors that permit them to resell our products and service offerings. Revenue resulting from our resellers and distributors accounted for approximately 49% of our total revenue in the year ended December 31, 2005, approximately 49% of our total revenue in the year ended December 31, 2006 and approximately 56% of our total revenue in the year ended December 31, 2007. For the years ended December 31, 2005, 2006 and 2007, no single reseller, distributor, customer or OEM accounted for more than ten percent of our total revenue. There is a risk that our pace of entering into such agreements may slow, or that our existing agreements may not produce as much business as we anticipate. There is also a risk that some or all of our resellers or distributors may be acquired, may change their business models or may go out of business, any of which could have an adverse effect on our business.

If we do not continue to establish and effectively manage our OEM relationships, our revenue could decline.

Our ability to sell our network security software products in new markets and to increase our share of existing markets will be impaired if we fail to expand our indirect distribution channels. Our sales strategy involves the establishment of multiple distribution channels domestically and internationally through strategic resellers, system integrators and OEMs. We have alliances with OEMs such as Nortel and Nokia and we cannot predict the extent to which these companies will be successful in marketing or selling our software. Our agreements with these companies could be terminated on short notice, and they do not prevent our OEMs, systems integrators, strategic resellers or other distributors from selling the network security software of other companies, including our competitors. Nortel and Nokia, or any other OEM, system integrator, strategic reseller or distributor, could give higher priority to other companies software or to their own software than they give to ours, which could cause our revenue to decline.

Our inability to effectively manage our expected headcount growth and expansion and our additional obligations as a public company could seriously harm our ability to effectively run our business.

Our historical growth has placed, and our intended future growth is likely to continue to place, a significant strain on our management, financial, personnel and other resources. We will likely not continue to grow at our historical pace due to limits on our resources. We have grown from 107 employees at December 31, 2004 to 240 employees at December 31, 2007. Since January 1, 2005, we have opened additional sales offices and have significantly expanded our operations. This rapid growth has strained our facilities and required us to lease additional space at our headquarters. In several recent quarters, we have not been able to hire sufficient personnel to keep pace with our growth. In addition to managing our expected growth, we have substantial additional obligations and costs as a result of becoming a public company in March 2007. These obligations include investor relations, preparing and filing periodic SEC reports, developing and maintaining internal controls over financial reporting and disclosure controls, compliance with corporate governance rules, Regulation FD and other requirements imposed on public companies by the SEC and the NASDAQ Global Market that we did not experience as a private company. Fulfilling these additional obligations will make it more difficult to operate a growing company. Any failure to effectively manage growth or fulfill our obligations as a public company could seriously harm our ability to respond to customers, the quality of our software and services and our operating results. To effectively manage growth and operate a public company, we are in the process of implementing an enterprise-wide information management system that includes new accounting, finance, management information and human resource systems and controls. Any failure by us to implement this system as planned, including any failure to adequately train personnel to use the new system, complete the implementation on schedule, complete the implementation within our budget or successfully transition our existing systems to the new system, could require us to devote significant additional management attention and financial resources, which could negatively affect the operation of our business.

The price of our common stock may be subject to wide fluctuations.

Prior to our IPO in March 2007, there was not a public market for our common stock. The market price of our common stock is subject to significant fluctuations. Among the factors that could affect our common stock price are the risks described in this Risk Factors section and other factors, including:

quarterly variations in our operating results compared to market expectations;

changes in expectations as to our future financial performance, including financial estimates or reports by securities analysts;

changes in market valuations of similar companies;

liquidity and activity in the market for our common stock;

actual or expected sales of our common stock by our stockholders;

strategic moves by us or our competitors, such as acquisitions or restructurings;

general market conditions; and

domestic and international economic, legal and regulatory factors unrelated to our performance.

Stock markets in general have experienced extreme volatility that has often been unrelated to the operating performance of a particular company. These broad market fluctuations may adversely affect the trading price of our common stock, regardless of our operating performance.

We and certain of our officers and directors have been named as co-defendants in, and are the subject of, certain legal proceedings which may result in substantial costs and divert management s attention and resources.

As described in Legal Proceedings below, multiple federal securities class action lawsuits have been filed naming our company and certain of our officers and directors as co-defendants. We are not able to predict the ultimate outcome of this litigation. It is possible that these matters could be resolved adversely to us, could result in substantial costs and could divert management s attention and resources, which could harm our business.

Risks associated with legal liability often are difficult to assess or quantify, and their existence and magnitude can remain unknown for significant periods of time. While we maintain director and officer insurance, the amount of insurance coverage may not be sufficient to cover a claim, and the continued availability of this insurance cannot be assured. We may in the future be the target of additional proceedings, and these proceedings may result in substantial costs and divert management s attention and resources.

Sales of substantial amounts of our common stock in the public markets, or the perception that they might occur, could reduce the price that our common stock might otherwise attain.

As of February 25, 2008, we had 24,647,719 outstanding shares of common stock. This number includes 6,185,500 shares of our common stock that we sold in our IPO, which has been and may in the future be resold at any time in the public market. This number also includes an aggregate of approximately 12.0 million shares held by directors, officers and venture capital funds that invested in Sourcefire prior to our initial public offering, and who may sell such shares at their discretion subject to certain volume limitations. Sales of substantial amounts of our common stock in the public market, as a result of the exercise of registration rights or otherwise, or the perception that such sales could occur, could adversely affect the market price of our common stock and may make it more difficult for you to sell your common stock at a time and price that you deem appropriate.

As a result of becoming a public company, we are obligated to develop and maintain proper and effective internal controls over financial reporting and are subject to other requirements that will be burdensome and costly. We may not complete our analysis of our internal controls over financial reporting in a timely manner, or these internal controls may not be determined to be effective, which may adversely affect investor confidence in our company and, as a result, the value of our common stock.

Beginning with our Annual Report on Form 10-K for the year ending December 31, 2008, we will be required, pursuant to Section 404 of the Sarbanes-Oxley Act of 2002 (Section 404), to furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting. This assessment will need to include disclosure of any material weaknesses identified by our management in our internal control over financial reporting. Our auditors may also be required to issue an attestation report on the effectiveness of our internal controls over financial reporting for the year ended December 31, 2008.

We are continuing the challenging process of compiling the system and processing documentation before we perform the evaluation needed to comply with Section 404. We may not be able to complete our evaluation, testing and any required remediation in a timely fashion. During the evaluation and testing process, if we identify one or more material weaknesses in our internal control over financial reporting, we will be unable to assert that our internal control is effective. If we are unable to assert that our internal control over financial reporting is effective, or if our auditors are unable to attest that our internal control over financial reporting is effective, we could lose investor confidence in the accuracy and completeness of our financial reports, which could have a material adverse effect on the price of our common stock. Failure to comply with these rules might make it more difficult for us to obtain certain types of insurance, including director and officer liability insurance, and we might be forced to accept reduced policy limits and coverage and/or incur substantially higher costs to obtain the same or similar coverage. The impact of these events could also make it more difficult for us to attract and retain qualified persons to serve on our board of directors, on committees of our board of directors, or as executive officers.

In addition, as a public company, we have and will continue to incur significant additional legal, accounting and other expenses that we did not incur as a private company, and our administrative staff has been and will continue to be required to perform additional tasks. For example, we have created and/or revised the roles and duties of our board committees, adopted disclosure controls and procedures, retained a transfer agent and adopted an insider trading policy and bear all of the internal and external costs of preparing and distributing periodic public reports in compliance with our obligations under the securities laws. In addition, changing laws, regulations and standards relating to corporate governance and public disclosure, and related regulations implemented by the Securities and Exchange Commission and the NASDAQ Global Market, are creating uncertainty for public companies, increasing legal and financial compliance costs and making some activities more time-consuming. These laws, regulations and standards are subject to varying interpretations, in many cases due to their lack of specificity, and, as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. We intend to invest resources to comply with evolving laws, regulations and standards, and this investment may result in increased general and administrative expenses and a diversion of management s time and attention from revenue-generating activities to compliance activities. If our efforts to comply with new laws, regulations and standards differ from the activities intended by regulatory or governing bodies due to ambiguities related to practice, regulatory authorities may initiate legal proceedings against us and our business may be harmed.

Anti-takeover provisions in our charter documents and under Delaware law could make an acquisition of us, which may be beneficial to our stockholders, more difficult and may prevent attempts by our stockholders to replace or remove our current management.

Our amended and restated certificate of incorporation and our amended and restated bylaws, each of which became effective in March 2007 upon completion of our IPO, contain provisions that may delay or prevent an acquisition of us or a change in our management. These provisions include a classified board of directors, a prohibition on actions by written consent of our stockholders, and the ability of our board of directors to issue preferred stock without stockholder approval. In addition, because we are incorporated in Delaware, we are governed by the provisions of Section 203 of the Delaware General Corporation Law, which prohibits stockholders owning in excess of 15% of our outstanding voting stock from merging or combining with us. Although we believe these provisions collectively provide for an opportunity to receive higher bids by requiring potential acquirors to negotiate with our board of directors, they would apply even if the offer may be considered beneficial by some stockholders. In addition, these provisions may frustrate or prevent attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors, which is responsible for appointing the members of our management.

Item 1B. *UNRESOLVED STAFF COMMENTS*

Not applicable.

Item 2. *PROPERTIES*

Our principal executive offices are located in Columbia, Maryland. We also lease sales offices in Vienna, Virginia; Livonia, Michigan; Wokingham, United Kingdom; Tokyo, Japan; Singapore; Courbevoie Cedex, France; Hoofddorp, The Netherlands and Espoo, Finland. Our lease in Columbia, Maryland expires on May 31, 2010; our lease in Vienna, Virginia expires on January 31, 2012; our lease in Livonia, Michigan expires on August 31, 2008; our lease in Wokingham, United Kingdom expires on January 24, 2012; our lease in Singapore expires on September 30, 2008; our leases in Tokyo, Japan; Courbevoie Cedex, France; Hoofddorp, The Netherlands; and Espoo, Finland run month-to-month. We believe that our facilities are generally suitable to meet our needs for the foreseeable future; however, we will continue to seek additional space as needed to satisfy our growth.

Item 3. *LEGAL PROCEEDINGS*

Consolidated IPO Class Action Litigation

On May 8, 2007, a putative class action lawsuit was filed in the United States District Court for the District of Maryland, against the Company and certain of its officers and directors, captioned *Howard Katz v. Sourcefire, Inc., et al.*, Case No. 1:07-cv-01210-WMN. Since then, two other putative class action lawsuits were filed in the United States District Court of Maryland against the Company and certain of its officers and directors and other parties making similar allegations, captioned *Mark Reaves v. Sourcefire, Inc. et al*, Case No. 1:07-cv-01351-JFM and *Raveill v. Sourcefire, Inc. et al*, Case No. 1:07-cv-01425-WMN. In addition, a fourth putative class action lawsuit was filed in the United States District Court for the Southern District of New York against the Company and certain of its officers and directors and other parties making similar allegations, captioned *Barry Pincus v. Sourcefire, Inc., et al.*, Case No. 1:07-cv-04720-RJH. Pursuant to a stipulation of the parties, and an order entered on or about June 29, 2007, the United States District Court of the Southern District of New York has transferred the *Pincus* case to the United States District Court for the District of Maryland.

These actions claim to be filed on behalf of all persons or entities who purchased the Company s common stock pursuant to an allegedly false and misleading registration statement and prospectus issued in connection with the Company s March 9, 2007 initial public offering (the IPO). These lawsuits allege violations of Section 11, Section 12 and Section 15 of the Securities Exchange Act of 1933, as amended, in connection with allegedly material misleading statements and/or omissions contained in the Company s registration statement and prospectus issued in connection with the IPO. The plaintiffs seek, among other things, a determination of class action status, compensatory and rescission damages, a rescission of the initial public offering, as well as fees and costs on behalf of a putative class.

On September 4, 2007, the Court granted a motion to consolidate the four putative class action lawsuits into a single civil action. In that same order, the Court also appointed Sandra Amrhein as lead plaintiff, the law firm of Kaplan Fox & Kilsheimer LLP as lead counsel, and Tydings & Rosenberg LLP as liaison counsel. On October 4, 2007, Ms. Amrhein filed an Amended Consolidated Class Action Complaint asserting legal claims that previously had been asserted in one or more of the four original actions.

On November 20, 2007, the defendants moved to dismiss the Amended Consolidated Class Action Complaint. The parties are currently in the process of briefing that motion to dismiss; no hearing date on those motions has been set by the Court.

From time to time, we are involved in other disputes and litigation in the normal course of business.

Item 4. *SUBMISSION OF MATTERS TO A VOTE OF SECURITY HOLDERS*

No matters were submitted to a vote of security holders during the fourth quarter of the fiscal year covered by this report.

PART II

Item 5. *MARKET FOR REGISTRANT S COMMON EQUITY, RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES*

Market Information

Our common stock is publicly traded on the NASDAQ Global Market under the symbol FIRE. Our stock began trading on the NASDAQ Global Market on March 9, 2007. The following table sets forth, for the periods indicated, the high and low sales prices of our common stock as reported by the NASDAQ Global Market.

	High	**Low**
Year ended December 31, 2007:		
First Quarter (from March 9, 2007)	**$ 18.83**	**$ 14.75**
Second Quarter	**$ 17.61**	**$ 10.71**
Third Quarter	**$ 15.00**	**$ 7.96**
Fourth Quarter	**$ 10.50**	**$ 7.23**

As of February 25, 2008, there were approximately 144 holders of record of our common stock. The number of holders of record of our common stock does not reflect the number of beneficial holders whose shares are held by depositories, brokers or other nominees.

Dividend Policy

We have never declared or paid any cash dividends on our common stock. We currently intend to retain all available funds and any future earnings for use in the operation and expansion of our business and do not anticipate paying any cash dividends in the foreseeable future.

Stock Performance Graph

The following graph illustrates a comparison of the total cumulative stockholder return on our common stock (traded under the symbol FIRE) since March 9, 2007, the date our stock commenced public trading, through December 31, 2007 to two indices: the Russell 2000 Index and the RDG Software Composite Index. The graph assumes an initial investment of $100 on March 9, 2007. The comparisons in the graph are required by the Securities and Exchange Commission and are not intended to forecast or be indicative of possible future performance of our common stock.

COMPARISON OF 9 MONTH CUMULATIVE TOTAL RETURN*
Among Sourcefire, Inc., The Russell 2000 Index
And The RDG Software Composite Index

* $100 invested on 3/9/07 in stock or 2/28/07 in index-including reinvestment of dividends. Fiscal year ending December 31.

3/9/07	3/07	4/07	5/07	6/07	7/07	8/07	9/07	10/07	11/07
100.00	113.75	77.28	88.27	90.32	78.44	61.85	58.62	63.27	52.36
100.00	101.07	102.89	107.10	105.53	98.32	100.54	102.27	105.20	97.65
100.00	101.26	106.17	110.27	107.74	104.49	105.72	110.02	124.97	114.33

Use of Proceeds

In March 2007, we completed the initial public offering of shares of our common stock. On March 9, 2007, we offered and sold 5,320,000 shares of our common stock, and certain of our stockholders offered and sold an aggregate of 450,000 shares of our common stock at a public offering price of $15.00 per share. The offer and sale of these shares were registered under the Securities Act of 1933, as amended, pursuant to our Registration Statement on Form S-1, as amended (File No. 333-138199), which was declared effective by the SEC on March 8, 2007. The managing underwriters of this offering were Morgan Stanley & Co. Incorporated, Lehman Brothers Inc., UBS Securities LLC and Jefferies & Company. On March 23, 2007, we offered and sold an additional 865,500 shares of our common stock at a price of $15.00 per share pursuant to the underwriters exercise in full of their over-allotment option.

Our portion of the net proceeds from the initial public offering was approximately $83.9 million after deducting underwriting discounts and commissions of approximately $1.05 per share, or $6.5 million in the aggregate, and $2.4 million in offering expenses. We did not receive any proceeds for the sale of the 450,000 shares by selling stockholders.

We intend to use the net proceeds from the offering for working capital and other general corporate purposes, including financing our growth, developing new products and funding capital expenditures. Pending such usage, we have invested the net proceeds in short-term, interest-bearing investment grade securities.

Item 6. *SELECTED FINANCIAL DATA*

The consolidated statement of operations data for the three years ended December 31, 2007 and the consolidated balance sheet data as of December 31, 2006 and 2007 have been derived from our audited consolidated financial statements appearing elsewhere in this report. The consolidated statement of operations data for the years ended December 31, 2003 and 2004 and the consolidated balance sheet data as of December 31, 2003, 2004 and 2005 have been derived from our audited consolidated financial statements that do not appear in this report. The selected consolidated financial data set forth below should be read in conjunction with Management s Discussion and Analysis of Financial Condition and Results of Operations set forth below and our consolidated financial statements and related notes included elsewhere in this report. The historical results are not necessarily indicative of the results to be expected in any future period.

	Year Ended December 31,				
	2007	**2006**	**2005**	**2004**	**2003**
	(In thousands, except share, per share and other operating data)				
Consolidated statement of operations data:					
Revenue:					
Products	34,332	30,219	23,589	12,738	8,153
Services	21,527	14,707	9,290	3,955	1,328
Total revenue	55,859	44,926	32,879	16,693	9,481
Cost of revenue:					
Products	9,523	8,440	6,610	4,533	2,570
Services	3,360	2,632	1,453	872	436
Total cost of revenue	12,883	11,072	8,063	5,405	3,006
Gross profit	42,976	33,854	24,816	11,288	6,475
Operating expenses:					
Research and development	11,902	8,612	6,831	5,706	3,751
Sales and marketing	25,860	20,652	17,135	12,585	9,002
General and administrative	10,599	5,017	5,120	2,905	2,141
Depreciation and amortization	1,649	1,230	1,103	752	441
In-process research and development	2,947				
Total operating expenses	52,957	35,511	30,189	21,948	15,335
Loss from operations	(9,981)	(1,657)	(5,373)	(10,660)	(8,860)
Other income (expense), net	4,604	792	(85)	164	16
Loss before income taxes	(5,377)	(865)	(5,458)	(10,496)	(8,844)
Income tax expense	(244)	(67)			
Net loss	(5,621)	(932)	(5,458)	(10,496)	(8,844)
Accretion of preferred stock	(870)	(3,819)	(2,668)	(2,451)	(1,262)

Net loss attributable to common stockholders	(6,491)	(4,751)	(8,126)	(12,947)	(10,106)
Net loss attributable to common stockholders per common share:					
Basic and diluted	(0.32)	(1.40)	(2.54)	(4.97)	(4.69)
Shares used in per common share calculations:					
Basic and diluted	20,434,792	3,389,527	3,200,318	2,602,743	2,156,725

	Year Ended December 31,				
	2007	2006	2005	2004	2003
	(In thousands, except share, per share and other operating data)				
Other operating data:					
Number of sales in excess of $500,000	15	14	9	5	2
Number of new 3D customers	266	273	149	136	161
Cumulative number of Fortune 100 3D customers at end of period	29	26	24	17	10
Number of full-time employees at end of period	240	182	135	107	84

Consolidated Balance Sheet Data

	Year Ended December 31,				
	2007	2006	2005	2004	2003
Cash and cash equivalents	33,071	13,029	1,106	3,563	5,315
Held-to-maturity investments	73,956	13,293	2,005	5,751	
Total assets	141,678	49,952	21,250	20,016	10,316
Long-term debt		1,312	990	461	345
Total liabilities	32,484	22,104	16,340	10,177	5,166
Total convertible preferred stock		66,747	40,007	37,339	19,958
Total stockholders equity (deficit)	109,194	(38,899)	(35,097)	(27,500)	(14,808)

Item 7. *MANAGEMENT S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS*

Introduction

Management s discussion and analysis of financial condition, changes in financial condition and results of operations is provided as a supplement to the accompanying consolidated financial statements and notes to help provide an understanding of Sourcefire, Inc. s financial condition and results of operations. This item of our Annual Report on Form 10-K is organized as follows:

Overview. This section provides a general description of our business, the performance indicators that management uses in assessing our financial condition and results of operations, and anticipated trends that management expects to affect our financial condition and results of operations.

Results of Operations. This section provides an analysis of our results of operations for the three years ended December 31, 2007.

Liquidity and Capital Resources. This section provides an analysis of our cash flows for the year ended December 31, 2007 and a discussion of our capital requirements and the resources available to us to meet those requirements.

Critical Accounting Policies and Estimates. This section discusses accounting policies that are considered important to our financial condition and results of operations, require significant judgment or require estimates on the part of management in application. Our significant accounting policies, including those considered to be critical accounting policies, are summarized in Note 2 to the accompanying consolidated financial statements.

Overview

We are a leading provider of Enterprise Threat Management (ETM) solutions for information technology (IT) infrastructures of commercial enterprises (e.g., healthcare, financial services, manufacturing, energy, education, retail, telecommunications) and federal and state government organizations. The Sourcefire 3D^{tm} System comprised of multiple Sourcefire hardware and software product offerings provides a comprehensive, intelligent network defense that unifies intrusion prevention system (IPS), network behavior analysis (NBA), network access control (NAC) and vulnerability assessment (VA) solutions under a common management framework. This ETM approach equips our customers with an efficient and effective layered security defense protecting computer network assets before, during and after an attack.

We sell our network security solutions to a diverse customer base that includes 29 of the Fortune 100 and over half of the 30 largest U.S. government agencies. We also manage two of the security industry s leading open source initiatives, Snort and ClamAV.

2007 Developments

Initial Public Offering

In March 2007, we completed the initial public offering, or IPO, of our common stock in which we sold and issued 6,185,500 shares of our common stock, including 865,500 shares sold by us pursuant to the underwriters full exercise of their over-allotment option, at an issue price of $15.00 per share. We raised a total of $92.8 million in gross proceeds from the IPO, or approximately $83.9 million in net proceeds after deducting underwriting discounts and commissions of $6.5 million and other offering costs of $2.4 million. Upon the closing of the IPO, all shares of convertible preferred stock outstanding automatically converted into an aggregate of 14,302,056 shares of common stock.

Acquisition of ClamAV

In August 2007, we closed on our acquisition of the intellectual property assets of ClamAV, an open source gateway anti-virus and anti-malware project. We paid $3.5 million in cash to the former owners, and deposited an additional $1.0 million in cash into escrow, to be paid to the sellers upon the delivery of certain additional source code, which is currently expected to be completed in the first quarter of 2008. We allocated $2.9 million of the purchase price to in-process research and development and allocated the remaining $634,000 to certain marketing related intangible assets. The estimated fair value of the in-process research and development project was determined by the use of a discounted cash flow model, using a discount rate that took into account the stage of completion and the risks surrounding the successful development and commercialization of the technology and product. The amount allocated to in-process research and development was immediately expensed, as there is no anticipated alternative future use for the acquired technology. The estimated fair value of the marketing-related intangible assets was determined using the relief from royalty method. As of December 31, 2007, we determined that it was probable that the additional source code would be completed in 2008 and the contingent payment would be made; therefore, the $1.0 million placed into escrow was accrued as a liability and recorded as a compensation expense as the sellers are now our employees and the payment is for services rendered.

Key Financial Metrics and Trends

Pricing and Discounts

We maintain a standard price list for all of our products. Additionally, we have a corporate policy that governs the level of discounts our sales organization may offer on our products, based on factors such as transaction size, volume of products, federal or state programs, reseller or distributor involvement and the level of technical support commitment. Our total product revenue and the resulting cost of revenue and gross profit percentage are directly affected by our ability to manage our product pricing policy. Although to date we have not experienced pressure to reduce our prices, competition is increasing and, in the future, we may be forced to reduce our prices to remain competitive.

Revenue

We currently derive revenue from product sales and services. Product revenue is principally derived from the sale of our network security solutions. Our network security solutions include a perpetual software license bundled with a third-party hardware platform. Services revenue is principally derived from technical support and professional services. We typically sell technical support to complement our network security product solutions. Technical support entitles a customer to product updates, new rule releases and both telephone and web-based assistance for using our products. Our professional services revenue includes optional installation, configuration and tuning (network security deployment services). These network security deployment services typically occur on-site after delivery has occurred.

Product sales are typically recognized as revenue at shipment of the product to the customer, whether sold directly or through resellers. For sales made through distributors and original equipment manufacturers, or OEMs, we do not recognize revenue until we receive the monthly sales report which indicates the sell-through volume to end user customers. Revenue from services is recognized when the services are performed. For technical support services, revenue is recognized ratably over the term of the support arrangement, which is usually a 12-month agreement providing for payment in advance and automatic renewals as evidenced by customer payment.

We sell our network security solutions globally. However, 81% of our revenue for 2006 and 75% of our revenue for 2007 was generated by sales to U.S.-based customers. We expect that our revenue from customers based outside of the United States will increase in amount and as a percentage of total revenue as we strengthen our international presence. We also expect that our revenue from sales through OEMs and distributors will increase in amount and as a percentage of total revenue as we expand such relationships.

Revenue from product sales has historically been highly seasonal, with more than one-third of our total product revenue in recent fiscal years generated in the fourth quarter and more than 60% in the second half of the year. The timing of our year-end shipments could materially affect our fourth quarter product revenue in any fiscal year and sequential quarterly comparisons. Revenue from our government customers has occasionally been influenced by the September 30th fiscal year-end of the U.S. federal government, which has historically resulted in our revenue from government customers being highest in the third quarter. Although we do not expect these general seasonal patterns to change substantially in the future, our revenue within a particular quarter is often affected significantly by the unpredictable procurement patterns of our customers. Our prospective customers usually spend a long time evaluating and making purchase decisions for network security solutions. Historically, many of our customers have not finalized their purchasing decisions until the final weeks or days of a quarter. We expect these purchasing patterns to continue in the future. Therefore, a delay in even one large order beyond the end of the quarter could materially reduce our anticipated revenue for a quarter. Because many of our expenses must be incurred before we expect to generate revenue, delayed orders could negatively impact our results of operations for a particular period and cause us to fail to meet the financial performance expectations of securities industry research analysts or investors.

Cost of Revenue

Cost of product revenue includes the cost of the hardware platform bundled into our network security solution, royalties for third-party software included in our network security solution, materials and labor that are incorporated in the quality assurance of our products, logistics, warranty, shipping and handling costs and, in the limited instance where we lease our network security solutions to our customers, depreciation and amortization. For the years ended December 31, 2007 and 2006, cost of product revenue was 28% of total product revenue for both periods. Hardware costs, which are our most significant cost item, generally have not fluctuated materially as a percentage of revenue in recent years because competition among hardware platform suppliers has remained strong and, therefore, per unit hardware cost has remained consistent. Because of the competition among hardware suppliers and our outsourcing of the manufacture of our products to three separate domestic contract manufacturers, we currently have no reason to expect that our cost of product revenue as a percentage of total product revenue will change significantly in the foreseeable future due to hardware pricing increases. However, hardware or other costs of manufacturing may increase in the future. We incur labor and associated overhead expenses, such as occupancy costs and fringe benefits costs, as part of managing our outsourced manufacturing process. These costs are included as a component of our cost of product revenue, but they have not been material to date.

Cost of services revenue includes the direct labor costs of our employees and outside consultants engaged to furnish those services, as well as their travel and associated direct material costs. Additionally, we include in cost of services revenue an allocation of overhead expenses such as occupancy costs, fringe benefits and supplies as well as the cost of time and materials to service or repair the hardware component of our products covered under a renewed support arrangement beyond the manufacturer s warranty. For the years ended December 31, 2007 and 2006, cost of services revenue was 16% and 18%, respectively, of total services revenue. We anticipate incurring an increasing amount of these services costs in the future for additional personnel to support and service our growing customer base.

Gross Profit

Our gross profit is affected by a variety of factors, including competition, the mix and average selling prices of our products, our pricing policy, technical support and professional services, new product introductions, the cost of hardware platforms, the cost of labor to generate such revenue and the mix of distribution channels through which our products are sold. Although we have not had to reduce the prices of our products or vary our pricing policy in recent years, our gross profit would be adversely affected by price declines if we are unable to reduce costs on existing products and fail to introduce new products with higher margins. Currently, product sales typically have a lower gross profit as a percentage of revenue than our services due to the cost of the hardware platform. Our gross profit for any particular quarter could be adversely affected if we do not complete a sufficient level of sales of higher-margin products by the end of the quarter. As discussed above, many of our customers do not finalize purchasing decisions until the final weeks or days of a quarter, so a delay in even one large order of a higher-margin product could reduce our total gross profit percentage for that quarter. For the years ended December 31, 2007 and 2006, gross profit was 77% and 75%, respectively, of total revenue. Based on current market conditions, we do not expect these percentages to change significantly in the foreseeable future, although unexpected pricing pressures or an increase in hardware or other costs would cause our gross profit percentage to decline.

Operating Expenses

Research and Development. Research and development expenses consist primarily of payroll, benefits and related occupancy and other overhead for our engineers, costs for professional services to test our products, and costs associated with data used by us in our product development.

We have significantly expanded our research and development capabilities and expect to continue to expand these capabilities in the future. We are committed to increasing the level of innovative design and development of new products as we strive to enhance our ability to serve our existing commercial and federal government markets as well as new markets for security solutions. To meet the changing requirements of our customers, we will need to fund investments in several development projects in parallel. Accordingly, we anticipate that our research and development expenses will continue to increase in absolute dollars for the foreseeable future, but should decline moderately as a percentage of total revenue as we expect to grow our revenues more rapidly than our research and development expenditures. For the years ended December 31, 2007 and 2006, research and development expense was $11.9 million and $8.6 million, or 21% and 19% of total revenue, respectively.

Sales and Marketing. Sales and marketing expenses consist primarily of salaries, incentive compensation, benefits and related costs for sales and marketing personnel; trade show, advertising, marketing and other brand-building costs; marketing consultants and other professional services; training, seminars and conferences; travel and related costs; and occupancy and other overhead costs.

As we focus on increasing our market penetration, expanding internationally and continuing to build brand awareness, we anticipate that selling and marketing expenses will continue to increase in absolute dollars, but decrease as a percentage of our revenue, in the future.

For the years ended December 31, 2007 and 2006, sales and marketing expense was $25.9 million and $20.7 million, or 46% of total revenue for both periods.

General and Administrative. General and administrative expenses consist primarily of salaries, incentive compensation, benefits and related occupancy and other overhead costs for executive, finance, information system, human resources and administrative personnel; legal, accounting and tax preparation and advisory fees; travel and related costs; information systems and infrastructure costs; and corporate insurance.

General and administrative expenses increased during the period of time leading up to our IPO and, as we operate as a public company, we have incurred additional expenses for costs associated with compliance with Section 404 of the Sarbanes-Oxley Act of 2002, directors and officers liability insurance, our investor relations function, and an increase in personnel to perform SEC reporting.

For the years ended December 31, 2007 and 2006, general and administrative expense was $10.6 million and $5.0 million, or 19% and 11% of total revenue, respectively.

In-process research and development costs. In-process research and development costs represent amounts allocated to acquired assets for which technological feasibility has not yet been reached and no alternative future use exists.

For the year ended December 31, 2007, in-process research and development costs were $2.9 million in connection with our acquisition of the assets of ClamAV. There was no corresponding expense during the same period in 2006.

Stock-Based Compensation. Effective January 1, 2006, we adopted the fair value recognition provisions of the Financial Accounting Standards Board s SFAS No. 123(R), Share-Based Payment, using the prospective transition method, which requires us to apply its provisions only to awards granted, modified, repurchased or cancelled after the effective date. Under this transition method, stock-based compensation expense recognized beginning January 1, 2006 is based on the grant date fair value of stock awards granted or modified after January 1, 2006.

As a result of adopting SFAS No. 123(R) on January 1, 2006, based on the estimated grant date fair value of employee stock options subsequently granted or modified, we recognized aggregate stock-based compensation expense of $2.6 million and $806,000 for the years ended December 31, 2007 and 2006, respectively. We use the Black-Scholes option pricing model to estimate the calculated value of granted stock options. The use of option valuation models requires the input of highly subjective assumptions, including the expected term and the expected stock price volatility.

Results of Operations

The following table sets forth our results of operations for the periods shown:

	Years Ended December 31		**Variance**		**Years Ended December 31**		**Variance**	
	2007	**2006**	**$**	**%**	**2006**	**2005**	**$**	**%**
Revenue:								
Products	$ 34,332	$ 30,219	$ 4,113	14%	$ 30,219	$ 23,589	$ 6,630	28%
Technical support and professional services	21,527	14,707	6,820	46%	14,707	9,290	5,417	58%
Total revenue	55,859	44,926	10,933	24%	44,926	32,879	12,047	37%
Cost of revenue:								
Products	9,523	8,440	1,083	13%	8,440	6,610	1,830	28%
Technical support and professional services	3,360	2,632	728	28%	2,632	1,453	1,179	81%
Total cost of revenue	12,883	11,072	1,811	16%	11,072	8,063	3,009	37%
Gross profit	42,976	33,854	9,122	27%	33,854	24,816	9,038	36%
Operating expenses:								
Research and development	11,902	8,612	3,290	38%	8,612	6,831	1,781	26%
Sales and marketing	25,860	20,652	5,208	25%	20,652	17,135	3,517	21%
	10,599	5,017	5,582	111%	5,017	5,120	(103)	(2)%

General and administrative								
Depreciation and amortization	1,649	1,230	419	34%	1,230	1,103	127	12%
In-process research and development costs	2,947		2,947	100%				0%
Total operating expenses	52,957	35,511	17,446	49%	35,511	30,189	5,322	18%
Loss from operations	(9,981)	(1,657)	(8,324)	(502)%	(1,657)	(5,373)	3,716	69%
Other income (expense), net	4,604	792	3,812	481%	792	(85)	877	1032%
Income (loss) before income taxes	(5,377)	(865)	(4,512)	(522)%	(865)	(5,458)	4,593	84%
Income tax expense	(244)	(67)	(177)	(264)%	(67)		(67)	N/A
Net Loss	$ (5,621)	$ (932)	$ (4,689)	(503)%	$ (932)	$ (5,458)	$ 4,526	83%

The following table sets forth our results of operations as a percentage of total revenue for the periods shown:

	Years Ended December 31		
	2007	2006	2005
Revenue:			
Products	61%	67%	72%
Technical support and professional services	39%	33%	28%
Total revenue	100%	100%	100%
Cost of revenue:			
Products	17%	19%	20%
Technical support and professional services	6%	6%	5%
Total cost of revenue	23%	25%	25%
Gross profit	77%	75%	75%
Operating expenses:			
Research and development	22%	19%	21%
Sales and marketing	46%	46%	52%
General and administrative	19%	11%	16%
Depreciation and amortization	3%	3%	3%
In-process research and development costs	5%	0%	0%
Total operating expenses	95%	79%	92%
Loss from operations	(18)%	(4)%	(17)%
Other income (expense), net	8%	2%	0%
Income (loss) before income taxes	(10)%	(2)%	(17)%
Income tax expense	0%	0%	0%
Net Loss	(10)%	(2)%	(17%)

Comparison of Years Ended December 31, 2007 and 2006

Revenue. Our total revenue increased 24% to $55.9 million in the year ended December 31, 2007 from $44.9 million in the year ended December 31, 2006. Product revenue increased 14% to $34.3 million in the year ended December 31, 2007 from $30.2 million in the year ended December 31, 2006. The increase in product revenue was driven primarily by higher demand for our sensor products, sales of which increased $3.4 million, including $1.1 million of sales from our 9800 sensors introduced in the fourth quarter. In addition, royalty income increased $1.1 million. These increases were partially offset by a decrease in sales of our software only license products of $1.0 million. Our services revenue increased 46% to $21.5 million in the year ended December 31, 2007 from $14.7 million in the year ended December 31, 2006. The increase in services revenue resulted from our support services being provided to a larger installed customer base comprised of new customers, as well as current customers who renewed their maintenance subscriptions.

Cost of Revenue. Total cost of revenue increased 16% to $12.9 million in the year ended December 31, 2007 from $11.1 million in the year ended December 31, 2006. Product cost of revenue increased 13% to $9.5 million in the year ended December 31, 2007 from $8.4 million in the year ended December 31, 2006. During the year ended December 31, 2007, we did not experience a material increase in our cost per unit of hardware platforms, which is the largest component of our product cost of revenue. The increase in product cost of revenue was driven primarily by higher volume demand for our sensor products, for which we must procure and provide the hardware platform to our customers. Our services cost of revenue increased 28% to $3.4 million in the year ended December 31, 2007, compared to $2.6 million in the year ended December 31, 2006. This increase was attributable to our hiring of additional personnel to both service our larger installed customer base and to provide training and professional services to our customers.

Gross Profit. Gross profit increased 27% to $43.0 million in the year ended December 31, 2007 from $33.9 million in the year ended December 31, 2006. Gross profit as a percentage of total revenue increased to 77% in the year ended December 31, 2007 from 75% in the year ended December 31, 2006, primarily due to additional, higher-margin services revenues, which grew at a higher rate than our product revenues.

Research and Development. Research and development expenses increased 38% to $11.9 million, or 22% of total revenue, in the year ended December 31, 2007 from $8.6 million, or 19% of total revenue, in the year ended December 31, 2006. The increase in the amount of research and development expenses was primarily due to an increase in payroll, benefits and overhead expenses of $2.1 million, expensing of the $1.0 million escrow from the ClamAV acquisition for the anticipated completion of additional source code and an increase in stock-based compensation expense of $268,000 due to the hiring of additional personnel in our research and development department to support the release of updates and enhancements to our 3D products.

Sales and Marketing. Sales and marketing expenses increased 25% to $25.9 million, or 46% of total revenue, in the year ended December 31, 2007 from $20.7 million, or 46% of total revenue, in the year ended December 31, 2006. The increase in the amount of sales and marketing expenses was primarily due to an increase of $2.5 million in payroll and benefit expenses for additional sales and marketing personnel, an increase of $578,000 in sales travel and travel-related expenses, an increase of $644,000 for stock-based compensation expense and an increase of $639,000 for advertising, promotion, partner marketing programs and trade show expenses in support of our network security solutions.

General and Administrative. General and administrative expenses increased 111% to $10.6 million, or 19% of total revenue in the year ended December 31, 2007 from $5.0 million, or 11% of total revenue in the year ended December 31, 2006. This increase in general and administrative expense was primarily due to an increase of payroll and benefits of $1.3 million for personnel hired in our accounting, information technology, human resources and legal departments, an increase of $841,000 for stock-based compensation expense, an increase of $1.6 million in professional fees related to audit, tax and regulatory compliance, and an increase of $474,000 in insurance premiums primarily due to an increase in our D&O insurance coverage.

Depreciation and Amortization. Depreciation and amortization expense increased 34% to $1.6 million in the year ended December 31, 2007 from $1.2 million in the year ended December 31, 2006. These expenses increased principally due to amortization of leasehold improvements relating to our UK office, additional lab and testing equipment purchased for the engineering department and personal computers purchased for personnel hired since December 31, 2006.

In-process research and development costs. For the year ended December 31, 2007, charges for in-process research and development totaled $2.9 million with no corresponding expense in 2006. The charge in 2007 is attributable to the August 2007 acquisition of certain assets of ClamAV, for which technological feasibility had not yet been reached and no alternative future use existed.

Other income (expense). Other income (expense) increased $3.8 million to $4.6 million during the year ended December 31, 2007 from $792,000 in the year ended December 31, 2006. The increase was primarily due to an increase in interest and investment income as a result of higher cash balances resulting from our March 2007 IPO.

Provision for income taxes. The provision for income taxes was $244,000 for the year ended December 31, 2007 as compared to $67,000 for the year ended December 31, 2006. We record a valuation allowance to reduce our deferred tax assets to the amount of future tax benefit that is more likely than not to be realized. At December 31, 2007, our net deferred tax assets were fully reserved except for a $29,000 benefit expected to be available to offset foreign tax liabilities in the future. At December 31, 2006, our net deferred tax assets were fully reserved. The provision for income taxes of $244,000 for the year ended December 31, 2007 principally relates to foreign income taxes.

Comparison of Years Ended December 31, 2006 and 2005

Revenue. Our total revenue increased 37% to $44.9 million in the year ended December 31, 2006 from $32.9 million in the year ended December 31, 2005. Product revenue increased 28% to $30.2 million in the year ended December 31, 2006 from $23.6 million in the year ended December 31, 2005. We did not introduce any new products during 2006 nor did we change the prices of our products from 2005 to 2006. The increase in product revenue was driven primarily by higher demand for our network security solutions throughout both periods, specifically sales of our enterprise class 3D Sensor which increased $5.5 million during 2006. Our services revenue increased 58% to $14.7 million in the year ended December 31, 2006 from $9.3 million in the year ended December 31, 2005. The increase in services revenue resulted primarily from support services being provided to a larger installed customer base in the 2006 period.

Cost of Revenue. Our total cost of revenue increased 37% to $11.1 million in the year ended December 31, 2006, compared to $8.1 million in the year ended December 31, 2005. Our product cost of revenue increased 28% to $8.4 million in the year ended December 31, 2006, compared to $6.6 million in the year ended December 31, 2005. During these periods, we did not experience a material increase in our cost per unit of hardware platforms, which is the largest component of our product cost of revenue. The increase in product cost of revenue was driven primarily by higher volume demand for our network security solutions for which we must procure and provide the hardware platform to our customers. Our services cost of revenue increased 81% to $2.6 million in the year ended December 31, 2006, compared to $1.5 million in the year ended December 31, 2005. Of this increase, $620,000 was attributable to our hiring of additional personnel to both service our larger installed customer base and to provide training and professional services to our customers, and $190,000 was attributable to extending the service contracts with the manufacturers for the hardware platform included with our products for our installed base of customers.

Gross Profit. Gross profit increased 36% to $33.9 million in the year ended December 31, 2006, from $24.8 million in the year ended December 31, 2005. Gross profit as a percentage of total revenue was 75% in both the years ended December 31, 2006 and December 31, 2005. This percentage did not vary between the periods because our product mix, the selling prices of our products and our hardware platform costs remained relatively stable throughout both periods. The increase of $9.1 million in gross profit was primarily due to an increase in product sales and an increase in the number of customers that contracted with us for support arrangements.

Research and Development. Research and development expenses increased 26% to $8.6 million, or 19% of total revenue, in the year ended December 31, 2006 from $6.8 million, or 21% of total revenue, in the year ended December 31, 2005. The increase in the amount of research and development expenses was primarily due to an increase in payroll and benefits of $1.8 million in the year ended December 31, 2006, which resulted from adding personnel in our research and development department to support the release of updates and enhancements to our RNA, Intrusion Sensor, and Defense Center products. In addition, at the beginning of 2006, we began product development work on a new release of the Snort intrusion detection engine.

Sales and Marketing. Sales and marketing expenses increased 21% to $20.7 million, or 46% of total revenue, in the year ended December 31, 2006 from $17.1 million, or 52% of total revenue, in the year ended December 31, 2005. The increase in the amount of sales and marketing expenses was primarily due to an increase of $2.1 million in salaries and incentive compensation expense for additional sales personnel, as well as an increase of $0.4 million for stock compensation expense and $0.3 million in advertising and promotion expenses in support of our 3D marketing message for our network security solutions.

General and Administrative. General and administrative expenses decreased 2% to $5.0 million, or 11% of total revenue in the year ended December 31, 2006 from $5.1 million, or 16% of total revenue in the year ended December 31, 2005. During 2006, payroll and benefits increased $180,000 for personnel hired in our accounting, information technology, human resources and legal departments, stock compensation increased $280,000 due to the adoption of FAS 123R, and audit and tax consulting increased $110,000; however, these increases were offset by a reduction of $620,000 in legal fees associated with the planned merger with Check Point Software Technologies, Inc. that was negotiated in the summer and autumn of 2005 and withdrawn in March 2006.

Depreciation and Amortization. Depreciation and amortization expenses increased 12% to $1.2 million in the year ended December 31, 2006 from $1.1 million in the year ended December 31, 2005. These expenses increased principally because of additional personal computers purchased for personnel hired during 2006.

Seasonality

Our product revenue has tended to be seasonal. In our third quarter, we have historically benefited from the Federal government s fiscal year end purchasing activity. This increase has been partially offset by European sales, which have tended to decline significantly in the summer months due to the practice of many Europeans taking extended vacation time and delaying capital purchase activities until their return in the fall. We have historically generated a significant portion of product revenue in the fourth quarter due to the combination of increased activity in Europe, coupled with North American enterprise customers who often wait until the fourth quarter to extract favorable pricing terms from their vendors, including Sourcefire. The timing of these shipments could materially affect our year-end product revenue. Currently, we do not see any indication that these seasonal patterns will change significantly in the foreseeable future.

Quarterly Timing of Revenue

On a quarterly basis, we have usually generated the majority of our product revenue in the final month of each quarter. We believe this occurs for two reasons. First, many customers wait until the end of the quarter to extract favorable pricing terms from their vendors, including Sourcefire. Second, our sales personnel, who have a strong incentive to meet quarterly sales targets, have tended to increase their sales activity as the end of a quarter nears, while their participation in sales management review and planning activities are typically scheduled at the beginning of a quarter.

Liquidity and Capital Resources

Cash Flows

At December 31, 2007, we had cash, cash equivalents and held-to-maturity investments of $107.0 million, as compared to $26.3 million at December 31, 2006.

Net cash provided by operating activities of $2.9 million for the year ended December 31, 2007 was primarily comprised of $2.8 million of net non-cash related expenses, a $6.9 million increase in deferred revenue, a $4.4 million increase in accounts payable and accrued expenses and $2.9 million of in-process research and development costs, offset by a $5.6 million net loss, a $4.1 million increase in accounts receivable, a $2.8 million increase in inventory and a $2.0 million increase in prepaid expenses and other assets.

Net cash used in investing activities of $66.9 million for the year ended December 31, 2007 was primarily comprised of a $125.1 million cash outlay for the purchase of held-to-maturity investments, a $3.1 million cash outlay for capital additions and a $4.6 million cash outlay for the acquisition of ClamAV, $1.0 million of which was paid into escrow, offset by $65.9 million of proceeds from the maturities of held-to-maturity investments. The capital additions were used for leasehold improvements to our U.K. office space and computer and network equipment for additional personnel.

Net cash provided by financing activities of $84.0 million for the year ended December 31, 2007 was primarily comprised of $84.9 million of net cash proceeds of our IPO offset by a $1.4 million debt repayment.

Liquidity Requirements

We manufacture and distribute our products through contract manufacturers and OEMs. This approach provides us with the advantage of relatively low capital investment and significant flexibility in scheduling production and managing inventory levels. The majority of our products are delivered to our customers directly from our contract manufacturers. Accordingly, our contract manufacturers are responsible for purchasing and stocking the components required for the production of our products, and they invoice us when the finished goods are shipped. By leasing our office facilities, we also minimize the cash needed for expansion. Our capital spending is generally limited to leasehold improvements, computers, office furniture and product-specific test equipment.

Our short-term liquidity requirements through December 31, 2008 consist primarily of the funding of capital expenditures and working capital requirements. We believe that cash flow from operations will be sufficient to meet these short-term requirements. In the event that cash flow from operations is not sufficient, we expect to fund these amounts through the use of existing cash and investment resources.

Our long-term liquidity requirements consist primarily of obligations under our operating leases. We believe that cash flow from operations will be sufficient to meet these long-term requirements.

In addition, we may utilize cash resources, equity financing or debt financing to fund acquisitions or investments in complementary businesses, technologies or product lines.

Contractual Obligations

Our principal commitments consist of obligations under our equipment facility, leases for office space and minimum contractual obligations for services. The following table describes our commitments to settle contractual obligations in cash as of December 31, 2007 (in thousands):

		Payments Due by Period		
	Total	**Less than One Year**	**1-3 Years**	**3-5 Years**
Operating Leases	$ 4,371	$ 1,529	$ 2,260	$ 582
Purchase Commitments(1)	7,639	7,639		

(1) We entered into a purchase commitment with a hardware manufacturing vendor with whom we have a current arrangement. Under the terms of this commitment, we have agreed to purchase a fixed quantity of inventory over an 18-month period. The value of the purchase commitment is approximately $800,000 of which $340,000 has been purchased to date. Additionally, we purchase components from a variety of suppliers and use several contract manufacturers to provide manufacturing services for our products. During the normal course of business, in order to manage manufacturing lead times and help ensure adequate component supply, we enter into agreements with contract manufacturers and suppliers that allow them to procure inventory based upon information provided by us. In certain instances, these agreements allow us the option to cancel, reschedule, and adjust our requirements based on our business needs prior to firm orders being placed. Consequently, a portion of our reported purchase commitments arising from these agreements are firm, non-cancelable, and unconditional commitments. As of December 31, 2007, we had total purchase commitments for inventory of approximately $7.2 million, exclusive of the commitment described above.

Critical Accounting Policies and Estimates

Our consolidated financial statements are prepared in accordance with accounting principles generally accepted in the United States of America. The preparation of these consolidated financial statements requires us to make estimates and assumptions that affect the reported amounts of assets, liabilities, revenue, costs and expenses and related disclosures. We evaluate our estimates and assumptions on an ongoing basis. Our actual results may differ from these estimates.

We believe that, of our significant accounting policies, which are described in Note 2 to our consolidated financial statements contained in this report, the following accounting policies involve a greater degree of judgment and complexity. Accordingly, we believe that the following accounting policies are the most critical to aid in fully understanding and evaluating our consolidated financial condition and results of operations.

Revenue Recognition. We recognize substantially all of our revenue in accordance with Statement of Position No. 97-2, Software Revenue Recognition, or SOP 97-2, as amended by SOP 98-4 and SOP 98-9. For each arrangement, we defer revenue recognition until: (a) persuasive evidence of an arrangement exists (e.g., a signed contract); (b) delivery of the product has occurred and there are no remaining obligations or substantive customer acceptance provisions; (c) the fee is fixed or determinable; and (d) collection of the fee is probable.

We allocate the total arrangement fee among each deliverable based on the fair value of each of the deliverables, determined based on vendor-specific objective evidence. If vendor-specific objective evidence of fair value does not exist for each of the deliverables, all revenue from the arrangement is deferred until the earlier of the point at which sufficient vendor-specific objective evidence of fair value can be determined for any undelivered elements or all elements of the arrangement have been delivered. However, if the only undelivered elements are elements for which we currently have vendor-specific objective evidence of fair value, we recognize revenue for the delivered elements based on the residual method.

We have established vendor-specific objective evidence of fair value for our technical support based upon actual renewals of each type of technical support that is offered and for each customer class. Technical support and technical support renewals are currently priced based on a percentage of the list price of the respective product or software and historically have not varied from a narrow range of values in the substantial majority of our arrangements. Revenue related to technical support is deferred and recognized ratably over the contractual period of the technical support arrangement, which ranges from 12 to 48 months in most arrangements. The vendor-specific objective evidence of fair value of our other services is based on the price for these same services when they are sold separately. Revenue for services that are sold either on a stand-alone basis or included in multiple element arrangements is deferred and recognized as the services are performed.

Changes in judgments and estimates about these assumptions could materially impact the timing of revenue recognition.

Accounting for Stock-Based Compensation. Effective January 1, 2006, we adopted the fair value recognition provisions of SFAS No. 123(R) using the prospective transition method, which requires us to apply its provisions only to awards granted, modified, repurchased or cancelled after the effective date. Under this transition method, stock-based compensation expense recognized beginning January 1, 2006 is based on the grant date fair value of stock awards granted or modified after January 1, 2006. As we had used the minimum value method for valuing our stock options under the disclosure requirements of Statement of Financial Accounting Standard (SFAS) No. 123, *Accounting for Stock Based Compensation* (SFAS No. 123), all options granted prior to January 1, 2006 continue to be accounted for under Accounting Principles Board Opinion No. 25, *Accounting for Stock Issued to Employees* (APB No. 25). Additionally, the pro forma disclosures that were required under the original provisions of SFAS No. 123 are no longer provided for outstanding awards accounted for under the intrinsic-value method of APB No. 25 beginning in periods after the adoption of SFAS No. 123(R).

Pursuant to SFAS 123(R), the fair value of each option grant is estimated on the date of grant using the Black-Scholes pricing model, which requires us to make assumptions as to volatility, risk-free interest rate, expected term of the awards, and expected forfeiture rate. The use of option valuation models requires the input of highly subjective assumptions, including the expected term and the expected stock price volatility. Additionally, the recognition of expense requires the estimation of the number of options that will ultimately vest and the number of options that will ultimately be forfeited.

Under the provisions of SFAS 123(R), the fair value of share-based awards is recognized as expense over the requisite service period, net of estimated forfeitures. We have assumed a forfeiture rate of 15% per annum for options and 10% per annum for restricted stock grants. We will record additional expense if the actual forfeiture rate is lower than estimated, and will record a recovery of prior expense if the actual forfeiture rate is higher than estimated. We rely on historical experience of employee turnover to estimate expected forfeitures.

Based on the estimated grant date fair value of employee stock options granted or modified, we recognized aggregate compensation expense of $1.9 million and $706,000 for the years ended December 31, 2007 and 2006, respectively. The following are the weighted average assumptions and fair values used in valuing the stock options granted and a discussion of our assumptions:

	2007	**2006**

Average risk-free interest rate	4.63%	4.68%
Expected dividend yield	0.0%	0.0%
Expected useful life	6.25 years	6.25 years
Expected volatility	74.8%	77.2%
Fair value of stock option awards granted during the year	$ 8.63	$ 5.47

Average risk-free interest rate This is the average U.S. Treasury rate (with a term that most closely resembles the expected life of the option) for the quarter in which the option was granted.

Expected dividend yield We have never declared or paid dividends on our common stock and do not anticipate paying dividends in the foreseeable future.

Expected useful life This is the period of time that the options granted are expected to remain outstanding. This estimate is derived from the average midpoint between the weighted average vesting period and the contractual term as described in the SEC s Staff Accounting Bulletin (SAB) No. 107, *Share-Based Payment*, as amended by SAB No. 111.

Expected volatility - Volatility is a measure of the amount by which a financial variable such as a share price has fluctuated (historical volatility) or is expected to fluctuate (expected volatility) during a period. Given our limited historical stock data from our initial public offering in March 2007, we have used a blended volatility to estimate expected volatility. The blended volatility includes the average of our preceding daily historical volatility from our initial public offering to the respective grant date and an average of our peer group preceding daily historical volatility consistent with the expected life of the option. Our peer group historical volatility includes the historical volatility of companies that are similar in revenue size, are in the same industry or are competitors.

If we had made different assumptions about the stock price volatility rates, expected life, expected forfeitures and other assumptions, the related compensation expense and net income could have been significantly different.

For options and other awards accounted for under SFAS 123(R), we recognize compensation expense on a straight-line basis over the requisite service period of the award.

The grant date aggregate fair value of options, net of estimated forfeitures, not yet recognized as expense as of December 31, 2007 was $4.5 million, which will be recognized over a weighted-average period of 2.45 years. To the extent the actual forfeiture rate is different from what we have anticipated; stock based compensation related to these awards will differ from our expectations. During 2007, we adjusted our estimated forfeiture rate for options from 10% to 15%.