TREND MICRO INC
Form 20-F
June 30, 2006

SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, DC 20549

FORM 20-F

(Mark One)

¨ **Registration statement pursuant to Section 12(b) or 12(g) of the Securities Exchange Act of 1934**

or

x **Annual report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the fiscal year ended December 31, 2005**

or

¨ **Transition report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934**

For the transition period from _____ to _____

Commission file number 333-10486

TREND MICRO KABUSHIKI KAISHA

(Exact Name of Registrant as Specified in Its Charter)

TREND MICRO INCORPORATED

(Translation of Registrant s Name Into English)

JAPAN

(Jurisdiction of Incorporation or Organization)

Shinjuku MAYNDS Tower, 1-1, Yoyogi 2-chome, Shibuya-ku, Tokyo

151-0053, Japan

(Address of Principal Executive Offices)

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

Title of Each Class	Name of Each Exchange on Which Registered
None	None

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

(1) Common Stock*

(Title of Class)

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:

None

(Title of Class)

Indicate the number of outstanding shares of each of the issuer s classes of capital or common stock as of the close of the period covered by the annual report.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.

Yes x No ¨

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934.

Yes x No ¨

Note Checking the box above will not relieve any registrant required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 from their obligations under those Sections.

As of December 31, 2005, 134,090,494 shares of common stock were outstanding, including 1,565,200 American Depositary Shares represented by 1,565,200 shares of common stock.

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 x No ¨

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

Large accelerated filer x Accelerated filer ¨ Non-accelerated filer ¨

Indicate by check mark which financial statement item the registrant has elected to follow.

Item 17 ¨ Item 18 x

All information contained in this report is as of December 31, 2005 or for the year ended December 31, 2005 unless the context otherwise indicates. In tables appearing in this annual report, figures may not add up to totals due to rounding.

* Not for trading, but only in connection with the registration of American Depositary Shares, each of which represents one share of Common Stock.

Cautionary Statement Regarding Forward-Looking Statements

This annual report on Form 20-F contains forward-looking statements within the meaning of the Section 21E of the Securities Exchange Act of 1934. To the extent that statements in this annual report do not relate strictly to historical or current facts, they may constitute forward-looking statements. These forward-looking statements are based upon management s current assumptions and beliefs in light of the information currently available to it, but involve known and unknown risks and uncertainties. Our actual actions or results may differ materially from those discussed in the forward-looking statements. We undertake no obligation to publicly update any forward-looking statement after the date of this annual report, but investors are advised to consult any further disclosures by us in our subsequent filings pursuant to the Securities Exchange Act of 1934.

Important risks and factors that could cause our actual results to differ materially from our expectations are generally set forth in Item 3.D of this annual report and include, without limitation:

- difficulties in addressing new virus and other computer security problems;
- timing of new product introductions and lack of market acceptance for our new products;
- the level of continuing demand for, and timing of sales of, our existing products;
- rapid technological change within the anti-virus software industry;
- changes in customer needs for anti-virus software;
- existing products and new product introductions by our competitors and the pricing of these products;
- declining prices for our products and services;
- the effect of future acquisitions on our financial condition and results of operations;
- the effect of adverse economic trends on our principal markets;
- the effect of foreign exchange fluctuations on our results of operations;
- an increase in the incidence of product returns;
- the potential lack of attractive investment targets;

difficulties in successfully executing our investment strategy; and

other risks discussed under Risk Factors and elsewhere in this annual report.

As used in this annual report, unless otherwise specified, references to Trend Micro are to Trend Micro Incorporated. Also, as used in this annual report, references to we , our and us are to Trend Micro Incorporated and, except as the context otherwise requires, its consolidated subsidiaries.

Also, as used in this annual report:

dollar or $ means the lawful currency of the United States of America, and yen or (Yen) means the lawful currency of Japan.

U.S. GAAP means generally accepted accounting principles in the United States.

ADS means an America Depositary Share, each representing 1 share of our common stock, and ADR means an American Depositary Receipt evidencing ADSs.

fiscal 2005 and fiscal year 2005 refer to our fiscal year ended December 31, 2005, and other fiscal years are referred to in a corresponding manner.

In tables appearing in this annual report, figures may not add up to totals due to rounding.

Item 1. Identify of Directors, Senior Management and Advisers.

Not applicable

Item 2. Offer Statistics and Expected Timetable.

Not applicable

Item 3. Key Information.

A. Selected Financial Data.

The selected financial data for the years ending December 31, 2003, 2004 and 2005, and as of December 31, 2004 and 2005 is derived from the Company s audited consolidated financial statements, which are included elsewhere in this Annual Report on Form 20-F. The historical statement of income information audited financial statements for the years ended December 31, 2001, 2002, 2003 and 2004 have been restated and the financial data presented below reflects the restatement as discussed in Note 2(1), Restatements to the consolidated financial statements. The historical restated consolidated following financial data for the years ended December 31, 2002 and 2001 has been derived from the consolidated unaudited financial statements not included herein and includes the effects of the restatement items discussed in Note 2, Restatements of the Notes to the Consolidated Financial Statements. Selected financial data should also be read in conjunction with Operating and Financial Review and Prospects included as Item 5 and the Consolidated Financial Statements and the related notes thereto which begin on page F-2 and are in response to Item 8 and Item 18.

	Year Ended December 31,					
	2001	2002	2003	2004	2005	2005
	(restated)	(restated)	(restated)	(restated)		
	(in millions of yen and thousands of dollars, except per share data)					
Net Sales	(Yen) 31,326	(Yen) 42,980	(Yen) 48,088	(Yen) 62,049	(Yen) 73,030	$ 618,897
Cost of sales: (1)						
Amortization of capitalized software, and Materials	1,899	2,354	3,168	3,236	2,599	22,022
Maintenance	854	1,806	2,194	2,261	1,671	14,163
Customer Support	2,449	3,858	4,831	5,724	6,858	58,118
Total Cost of sales	5,202	8,018	10,193	11,221	11,128	94,303
Operating expenses:(1)						
Selling	10,001	15,052	15,360	16,009	20,944	177,496
Research and development	1,901	1,700	1,725	2,597	4,395	37,247
General and administrative	4,453	4,344	5,656	6,144	8,991	76,192
Goodwill write-off	2,253					

Total operating expenses	18,608	21,096	22,741	24,750	34,330	290,935
Operating income	7,516	13,866	15,154	26,078	27,572	233,659
Other income (expense), net	241	(768)	175	247	1,536	13,022
Net income before tax	7,757	13,098	15,329	26,325	29,108	246,681
Income taxes	3,241	5,395	6,103	10,503	10,504	89,022
Income before minority interest and equity in earnings (losses) of affiliated companies	4,516	7,703	9,226	15,822	18,604	157,659
Minority interest in income of consolidated subsidiaries					(0)	(3)
Income from consolidated companies	4,516	7,703	9,226	15,822	18,604	157,656
Equity in earnings (losses) of affiliated companies	(130)	11	24	53	66	564
Net income	(Yen) 4,386	(Yen) 7,714	(Yen) 9,250	(Yen) 15,875	(Yen) 18,670	$ 158,220
Net income per share (basic)(2)	(Yen) 33.33	(Yen) 58.39	(Yen) 70.11	(Yen) 120.64	(Yen) 139.85	$ 1.19

	Year Ended December 31,					
	2001	2002	2003	2004	2005	2005
	(in millions of yen and thousands of dollars, except per share data)					
Net income per share (diluted)(2)	(Yen) 33.02	(Yen) 58.22	(Yen) 69.95	(Yen) 118.59	(Yen) 137.83	$ 1.17
Cash dividends per share(2)	(Yen)	(Yen)	(Yen)	(Yen) 14	(Yen) 36	$ 0.31
Weighted average common shares outstanding (basic)(2)	131,594,913	132,111,467	131,940,179	131,588,738	133,498,438	
Weighted average common shares outstanding (diluted)(2)	132,832,159	132,494,201	132,235,128	133,863,237	135,456,212	

(1) The Company has historically disclosed maintenance costs as part of the Research and development and maintenance line item within operating expenses in the consolidated statement of income. Starting fiscal year 2005, maintenance costs are included in cost of sales, therefore, prior years figures have been restated to reflect such amendment. In addition, customer support expenses, which were disclosed as a component of operating expenses, through December 31, 2004, have also been included in cost of sales starting fiscal year ended 2005, therefore, prior years figures have been restated to reflect such amendment. Refer to Note 2 to the consolidated financial statements, included elsewhere in this Annual Report for additional information.

(2) We effected a one-to-two stock split on May 18, 2001. The share and per share amounts for each of the year ended December 31, 2001 have been restated to reflect that stock split.

	Year Ended December 31,					
	2001	2002	2003	2004	2005	2005
	(in millions of yen and thousands of dollars, except per share data)					
Consolidated Balance Sheet Information						
Cash and cash equivalents	(Yen) 40,783	(Yen) 47,830	(Yen) 46,719	(Yen) 52,908	(Yen) 59,613	$ 505,191
Total assets	64,729	73,838	81,271	106,734	132,935	1,126,570
Current portion of long-term debt	3,000	5,000	6,500			
Long-term debt	11,500	6,500				
Total liabilities	33,963	36,694	37,319	43,559	51,068	432,776
Common stock	6,834	7,257	7,396	11,427	12,485	105,804
Shareholders equity	(Yen) 30,766	(Yen) 37,144	(Yen) 43,952	(Yen) 63,175	(Yen) 81,863	$ 693,755

Exchange Rates.

In this annual report, we have translated Japanese yen amounts into U.S. dollars solely for the convenience of readers. Unless otherwise indicated, the rate we used for the translation was (Yen) 118. 00 per $1, which was the approximate rate on December 31, 2005. The following table shows the noon buying rates for Japanese yen expressed in Japanese yen per $1. On June 15, 2006 the noon buying rate announced by the Federal Reserve Bank of New York was (Yen) 115.06 per $1.

Year ended/ending December 31,	High	Low	Average (1)	Period-end
2001	131.47	114.26	122.18	131.04
2002	134.77	115.71	124.81	118.75
2003	121.42	106.93	115.99	107.13
2004	114.30	102.56	108.15	102.68
2005	120.93	102.26	110.74	117.88
2006 (through June 15)	119.07	110.07	115.61	115.06
Calendar Year 2005				
December	120.93	115.78	118.46	117.88
Calendar Year 2006				
January	117.55	113.96	115.48	116.88
February	118.95	115.82	117.86	115.82
March	119.07	115.89	117.28	117.48
April	118.66	113.79	117.07	113.79
May	113.46	110.07	111.73	112.26
June (until June 15)	115.06	111.66	113.60	115.06

(1) For annual averages, calculated based on the average of the exchange rates on the last day of each month during the period. For monthly averages, calculated based on the average of noon buying rates.

B. Capitalization and Indebtedness.

Not applicable

C. Reasons for the Offer and Use of Proceeds.

Not applicable

D. Risk Factors.

The occurrence of any of the following risks could hurt our business, financial condition or results of operations. In such case, the trading price of our shares and the ADSs could decline and you could lose all or part of your investment. Other risks and uncertainties not now known to us or that we think are immaterial may also impair our business.

MAJOR SOFTWARE AND HARDWARE VENDORS MAY INCORPORATE ANTI-VIRUS PROTECTION IN THEIR PRODUCT OFFERINGS, WHICH COULD RENDER OUR PRODUCTS OBSOLETE OR UNMARKETABLE.

Major vendors of operating system software and other software such as firewall or e-mail software or computer hardware may decide to enhance or bundle their products with their other products to include anti-virus functions. These companies may offer anti-virus protection as a standard feature in their products, at minimal or no additional cost to customers. This could render our products obsolete or unmarketable, particularly if anti-virus products offered by these vendors were comparable or superior to our products. In addition, even if these vendors anti-virus products offered fewer functions than our products, or were less effective in detecting and cleaning virus-infected files, customers could still choose them over our products due to lower cost or for any other reasons.

Microsoft Corp., a major operating system vendor, has acquired some security vendors such as GeCAD Software Srl., an anti-virus software vendor in Romania. Microsoft Corp. announced that they would provide anti-virus products or services such as named Windows OneCare or Client Protection in 2006. At this time, we do not know the details of those services or products, but if in fact Microsoft launches those products or services, and/or, if anti-virus functions were to be included in its operating system products, this could have a material adverse effect on our business, financial condition and results of operations.

BECAUSE WE GENERATE SUBSTANTIALLY ALL OF OUR SALES FROM A SINGLE PRODUCT LINE, WE ARE VULNERABLE TO DECREASED DEMAND FOR SUCH PRODUCTS.

Unlike software companies with diversified product lines, we derive substantially all of our net sales from licensing and selling anti-virus software products. Although we have begun to offer more comprehensive network and internet security and management software and services, we expect anti-virus products to continue to account for the largest portion of our net sales for the foreseeable future. If the demand for, or the prices of, anti-virus products drop as a result of competition, technological changes or other factors such as lower growth or a contraction in the worldwide anti-virus software market, this could have a material adverse effect on our business, financial condition and results of operations.

DETERIORATION IN OUR RELATIONSHIP WITH SOFTBANK BB CORP. COULD RESULT IN A DECREASE IN SALES OF OUR PRODUCTS.

We depend on our relationship with SOFTBANK BB (formerly SOFTBANK COMMERCE CORP.), which has played an instrumental role in the development of our business in Japan. SOFTBANK BB also has close relationships with many resellers and systems integrators through which we sell our anti-virus software to corporate end users in Japan. An adverse change in our relationship with SOFTBANK BB would result in decreased sales to SOFTBANK BB and could disrupt our relationship with many resellers of our products. This could make it difficult for us to market our products in Japan. Sales to SOFTBANK BB totaled approximately (Yen)9.2 billion, or 19.1%, of our net sales in fiscal 2003, approximately (Yen)10.4 billion, or 16.8%, of our net sales in fiscal 2004 and approximately (Yen)10.6 billion, or 14.5%, of our net sales in fiscal 2005. Because of our dependence on SOFTBANK BB, the price of shares and ADSs could fall as a result of adverse events affecting SOFTBANK BB, even if the events do not relate directly to us.

OUR PRODUCTS MAY BECOME OBSOLETE BECAUSE RAPID TECHNOLOGICAL CHANGE REGULARLY OCCURS IN THE ANTI-VIRUS SOFTWARE MARKET.

The anti-virus software market is characterized by:

- rapid technological change;
- the proliferation of new and changing computer viruses;
- frequent product introductions and updates; and
- changing customer needs.

These characteristics of our market create significant risks and uncertainties for our business success. For example, our competitors might introduce anti-virus products that are technologically superior to our products. Additionally, new software operating system, network system or anti-virus software industry standards could emerge. Emerging trends in these systems and standards currently include applications distributed over the Internet and the use of a Web browser to access client-server systems. Our existing products might be incompatible with some or all of such standards. Our business, financial condition and results of operations could materially suffer unless we are able to respond quickly and effectively to these developments.

OUR HARDWARE-BASED PRODUCTS FACE MANUFACTURING AND INVENTORY RISKS.

We rely on a small number of third parties to manufacture some of our hardware-based products, such as the Trend Micro Network VirusWall described in Item 4.B. We expect our reliance on third-party manufacturers to become more important as the number of our hardware-based products increases. Reliance on third-party manufacturers involves a number of risks, including a lack of control over the manufacturing process and the potential absence or unavailability of adequate capacity. If any of our third-party manufacturers cannot or will not manufacture our products in required volumes in compliance with environmental and other regulations in the markets we serve, on a cost-effective basis, in a timely manner, or at all, we will have to secure additional manufacturing capacity. The unexpected loss of any of our manufacturers could disrupt our business. Furthermore, our hardware-based products contain critical components supplied by a single or a limited number of third parties. Any significant shortage of components or the failure of the third-party supplier to maintain or enhance these products could lead to cancellation of customer orders or delays in the placement of orders and adversely affect our financial condition and results of operation.

WE MAY NOT GENERATE EXPECTED RESULTS IN STRATEGIC ALLIANCES

Because we are mainly focusing our business on the field of anti-virus software and do not offer other security products such as firewalls, we actively pursue strategic alliances with other companies that allow us to provide customers with integrated or other new products and services derived from the alliances. In fiscal year 2004, we began to provide a third party URL filtering solution and have signed contracts with Cisco Systems to integrate network worm and virus outbreak prevention services with Cisco s products and services. To launch and provide such products and services, we may invest substantial cash and other resources in product developments, marketing promotions and support and maintenance activities. However we may not earn revenue successfully from alliances despite our efforts, and such alliance may be terminated or dissolved by various causes before generating revenue.

WE MAY NOT BE ABLE TO INCREASE OUR MARKET SHARE IN THE U.S. AND EUROPEAN MARKETS BECAUSE OUR COMPETITORS ARE MORE ESTABLISHED THAN WE ARE IN THESE MARKETS.

We believe that our share of the anti-virus software market in the U.S. and Europe is significantly smaller relative to the market shares of our principal competitors, despite the growth of our sales in these markets in fiscal 2004 and 2005. Because our competitors are already well-established in these key markets and have greater financial and other resources and brand recognition, we may not be able to compete effectively for market share. If this happens, we may not be able to increase sales or our market share in these markets, which could materially hurt the prospects for growth in our business.

Some of our major competitors have the following advantages over us in the U.S. and European markets:

- greater name recognition;
- more diversified product lines;
- larger customer bases; and
- significantly greater financial, technical, marketing and other resources.

As a result, as compared to us, our competitors may be able to:

- better withstand downturns in the anti-virus software market and in the computer software market in general;
- adapt more quickly to new or emerging technologies or changes in customer requirements; or
- more effectively and profitably market, sell and support their products.

WE MAY SUFFER A LOSS OF SALES AND MARKET SHARE IN OUR CORE JAPANSE MARKET IF OUR COMPETITORS ACHIEVE SUCCESS IN JAPAN.

Our major competitors, McAfee, Inc. and Symantec Corporation, are active in the Japanese anti-virus software market and have allocated significant resources to achieve success in the Japanese anti-virus software market. Although these competitors currently have smaller shares of the Japanese market than us, each has significantly greater financial, marketing and other resources than we do. Additionally, competition in our core Japanese market could intensify in the future if other competitors emerge. As a result of our competitors efforts, we may not be able to maintain our current leading market position in Japan in the future. Also, in order to respond effectively to increased competition, we may be required to devote more of our product development, marketing and other resources to the Japanese market, which could limit our ability to grow in other markets. A material loss of sales and market share in Japan as a result of our competitors success could have a material adverse effect on our business, financial condition and results of operations.

BECAUSE WE MAY ACQUIRE COMPANIES TO GROW OUR BUSINESS, FUTURE ACQUISITIONS MAY REDUCE OUR EARNINGS AND RESULT IN INCREASED COSTS IN OUR BUSINESS OPERATIONS.

In a rapidly changing industry, we occasionally review acquisition opportunities. Accordingly, we may seek to expand our business through acquisitions. Unlike some of our major competitors, we have limited experience in acquiring existing businesses. Future acquisitions could result in numerous risks and uncertainties, including:

- our inability to retain customers, suppliers and other important business relationships of an acquired business;
- difficulties in integrating an acquired company into Trend Micro, including the acquired company s operations, personnel, products and information systems;
- diversion of our management s attention from other business concerns; and
- adverse effects on our results of operations from acquisition-related charges, impairment of goodwill and purchased technology and possible recognition of impairment charge.

If we make such an acquisition using our stock, our current shareholders ownership interests will be diluted. Any of these factors could materially hurt our business, financial condition and results of operations.

For example, in 2000, we acquired ipTrend to start a new business selling a Linux based remotely managed server appliance solution to small and medium sized companies. However, ipTrend performed poorly and was liquidated in December 2001. Due to the liquidation of ipTrend, (Yen) 2.3 billion was booked as goodwill write-off in 2001.

IF HACKERS GAIN UNAUTHORIZED ACCESS TO OUR SYSTEMS, WE COULD SUFFER DISRUPTIONS IN OUR BUSINESS AND LONG-TERM DAMAGE TO OUR REPUTATION.

We may be more susceptible to problems caused by hackers than other software companies. As an anti-virus software company that delivers virus protection products over the Internet, hackers specifically target us in order to cause us to transmit computer viruses or interrupt the delivery of our anti-virus software monitoring and security services over the internet which could result in further interruptions. We could suffer substantial disruptions in our business and material damage to our reputation which could in turn result in a significant loss of our customers and other important business relationships. We could also incur costs for public relations efforts following attacks by hackers. Hacker activities could also force us to incur substantial costs to fix technical problems or result in hackers gaining access to our proprietary information.

WE FACE NEW RISKS RELATED TO OUR ANTI-SPAM AND ANTI-SPYWARE SOFTWARE PRODUCTS.

Our anti-spam and anti-spyware products may falsely identify emails or programs as unwanted spam or potentially unwanted programs, or alternatively fail to properly identify unwanted emails or programs, particularly as spam emails or spyware are often designed to circumvent anti-spam or spyware products. Parties whose emails or programs are blocked by our products may seek redress against us for labeling them as spammers or spyware, or for interfering with their business. In addition, false identification of emails or programs as unwanted spam or potentially unwanted programs may reduce the adoption of these products.

WE MUST EFFECTIVELY MANAGE OUR GROWTH.

Our business has grown rapidly. This growth has placed, and any future growth would continue to place, a significant strain on our limited personnel, management and other resources. Our ability to manage any future growth in our business will require us to:

attract, train, retain, motivate and manage new employees successfully;

effectively integrate new employees into our operations; and

continue to improve our operational, financial, management and information systems and controls.

If we continue to grow, our management systems currently in place may be inadequate or we may not be able to effectively manage our growth. In particular, we may be unable to:

provide effective customer service;

develop and deliver products in a timely manner;

implement effective financial reporting and control systems; and

exploit new market opportunities and effectively respond to competitive pressures.

WE SELL OUR PRODUCTS THROUGH INTERMEDIARIES WHO MAY NOT VIGOROUSLY MARKET OUR PRODUCTS, OR MAY RETURN OUR PRODUCTS.

We market substantially all of our products to end users through intermediaries, including distributors, resellers and value-added resellers. Our distributors sell other products that are complementary to, or compete with, our products. While we encourage our distributors to focus on our products, these distributors may give greater priority to products of other suppliers, including competitors . They may also return the products to us under certain circumstances.

OUR CUSTOMERS MAY CANCEL OR DELAY THEIR PURCHASES OF OUR PRODUCTS, WHICH COULD ADVERSELY AFFECT OUR BUSINESS.

Our products may be considered to be capital purchases by certain enterprise customers. Capital purchases are often uncertain and, therefore, are canceled or delayed if the customer experiences a downturn in its business prospects or as a result of unfavorable economic conditions. Any cancellation or delay could adversely affect our results of operations.

WEAK FINANCIAL CONDITIONS OF SOME OF OUR DISTRIBUTORS MAY ADVERSELY AFFECT OUR OPERATING RESULTS.

Some of our distributors are experiencing financial difficulties worldwide, which may adversely impact our collection of accounts receivable. We regularly review the collectibility and creditworthiness of our distributors to determine an appropriate allowance for doubtful receivables. Our uncollectible accounts could exceed our current or future allowance for doubtful receivables, which would adversely impact our operating results.

OUR RESULTS OF OPERATIONS MAY SUFFER IF WE ARE REQUIRED TO PAY SIGNIFICANT AMOUNTS OF PENALTY PAYMENTS PURSUANT TO THE TERMS OF OUR SERVICE LEVEL AGREEMENTS.

We guarantee a certain quality of product support to our customers through our service level agreements. Pursuant to the terms of these agreements, under some circumstances, we are required to make penalty payments to our customers. For example, if we fail to provide our customers a virus pattern file within two hours of our receipt of a virus from the customer, the terms of the agreement require us to make a penalty payment to the dissatisfied customer which may amount up to 100% of the initial sale price. We have established reserves based on our assumptions and estimates. However, our assumptions and estimates may be wrong and our actual total penalty payments could materially exceed our reserves and adversely affect our results of operations and financial condition.

WE RELY HEAVILY ON OUR MANAGEMENT AND TECHNICAL PERSONNEL, WHO MAY NOT REMAIN WITH US IN THE FUTURE.

We rely, and will continue to rely, on a number of key technical and management employees, including our Chief Executive Officer, Eva Yi-Fen Chen. While we require our employees to sign employment agreements, our employees are generally not otherwise subject to noncompetition covenants. If any of our key employees leave, our business, results of operations and financial condition could suffer.

FLUCTUATIONS IN OUR QUARTERLY FINANCIAL RESULTS COULD CAUSE THE MARKET PRICE FOR OUR SHARES AND OUR ADSs TO BE VOLATILE.

We believe that our quarterly financial results may fluctuate in ways that do not reflect the long-term trend of our future financial performance. It is likely that in some future quarterly periods, our operating results may be below the expectations of public market analysts and investors. In this event, the price of our shares and our ADSs could fall.

Factors which could cause our quarterly financial results to fluctuate include:

- timing of sales of our products and services due to customers budgetary constraints, seasonal buying patterns and our promotional activities;
- new product introductions by our competitors;

significant marketing campaigns, research and development efforts, employee hiring, and other capital expenditures by us to drive the growth of our business;

changes in customer needs for anti-virus software; and

changes in economic conditions in our major markets.

WEAKNESS IN THE JAPANESE ECONOMY MAY HURT OUR BUSINESS PERFORMANCE BECAUSE JAPAN IS OUR LARGEST MARKET.

While our sales in the US and Europe have increased in recent years, we remain significantly dependent on the Japanese market. Net sales in Japan accounted for approximately 42% of our net sales in fiscal 2003, approximately 41% in fiscal 2004 and approximately 40% in fiscal 2005. In the past three years, the Japanese economy has performed poorly due to a number of factors, including weak consumer spending and lower capital investment by Japanese companies. We believe the sluggish Japanese economy has hindered growth in our net sales during most of the last three fiscal years, although it has shown signs of recovering during the last several months. Because of our dependence on the Japanese market, any deterioration in the condition of the Japanese economy could negatively impact our net sales.

FOREIGN EXCHANGE FLUCTUATIONS COULD LOWER OUR RESULTS OF OPERATIONS BECAUSE WE EARN REVENUES DENOMINATED IN SEVERAL DIFFERENT CURRENCIES.

Our reporting currency is the Japanese yen and the functional currency of each of our subsidiaries is the currency of the country in which the subsidiary is domiciled. However, a significant portion of our revenues and operating expenses is denominated in currencies other than the Japanese yen, primarily the US dollar, euro and the New Taiwan dollar. As a result, appreciation or depreciation in the value of other currencies as compared to the Japanese yen could result in material transaction or translation gains or losses which could reduce our operating results. These negative effects from currency fluctuations could become more significant if we are successful in increasing our sales in markets outside of Japan. We do not currently engage in currency hedging activities.

BECAUSE OUR BUSINESS DEPENDS SIGNIFICANTLY ON INTELLECTUAL PROPERTY, INFRINGEMENT OF OUR INTELLECTUAL PROPERTY COULD HURT OUR BUSINESS.

Our success depends upon the development of proprietary software technology. We rely on a combination of contractual rights and patent, copyright, trademark and trade secret laws to establish and protect proprietary rights in our software. If we are unable to establish and protect these rights, our competitors may be able to use our intellectual property to compete against us. This could limit our growth and hurt our business. At present, our U.S. consolidated subsidiary holds seven issued US patents and our Taiwan consolidated subsidiary holds four issued U.S. patents. It is possible that no additional patents will be issued to us or any of our subsidiaries. In addition, our issued patents may not prevent other companies from competing with us. We also enter into confidentiality agreements with our employees and license agreements with our customers, and limit access to our proprietary information and its distribution. However, we cannot guarantee that any of these measures will discourage others from misappropriating our technology or independently developing similar technology.

PRODUCT LIABILITY CLAIMS ASSERTED AGAINST US IN THE FUTURE COULD HURT OUR BUSINESS.

Our products are designed to protect customers network systems and personal computers from damage caused by computer viruses. As a result, if a customer suffers damage from viruses, the customer could sue us on product liability or related grounds, claim damages for data loss or make other claims. Additionally, as viruses are constantly evolving, purchasers of our software products must regularly update the software they have purchased from us with virus protection files that we make available for download from our website. Should we fail to properly test these virus protection files and distribute a defective file, these files could cause damage to the personal computers of our customers who have downloaded a defective file. For example, a file that we distributed on April 23, 2005 for an approximately 90 minute-period caused the computers of those updating with the file to slow and, in some cases, shut down. Cases of our files damaging the computers or our customers could lead to significant damage to our reputation and customers could sue on product liability or related grounds. Furthermore, starting in 2001, we began selling hardware devices which could give rise to a higher incidence of product liability claims than we have up until now experienced. Our license agreements typically contain provisions, such as disclaimers of warranty and limitations of liability, which seek to limit our exposure to certain types of product liability claims. However, in some jurisdictions these provisions may not be enforceable on statutory, public policy or other grounds. We currently do not carry product liability insurance covering claims arising in the United States. Damage to our reputation or successful product liability or related claims brought against us could materially harm our business.

OUR BUSINESS FACES THE RISK OF INTERRUPTION FROM POWER SHORTAGES, EARTHQUAKES, OUTBREAK OF BIOLOGICAL VIRUSES AND OTHER HAZARDS.

We face a number of potential business interruption risks that are beyond our control. The State of California experienced intermittent power shortages in 2000, sharp increases in the cost of energy and even interruptions of service to some business customers. If power shortages continue to be a problem, our business may be materially adversely affected. Additionally, we may experience natural disasters that could

interrupt our business.

Tokyo, where our corporate headquarter is located, is near a major earthquake fault. The impact of a major earthquake on our facilities, infrastructure and overall operations is not known. There is no guarantee that an earthquake would not seriously disturb our entire business operations. We are largely uninsured for losses and business disruptions caused by an earthquake and other natural disasters.

In addition, many of the key countries and regions in which we operate have sustained negative economic impact from events such as the continued fear of future terrorist attacks and the outbreak of severe acute respiratory syndrome, or SARS. Prolonged continuation of these adverse factors may hurt our results of operations and financial condition.

WE MAY HAVE TO CONSTRAIN OUR BUSINESS ACTIVITIES TO AVOID BEING DEEMED AN INVESTMENT COMPANY UNDER THE US INVESTMENT COMPANY ACT OF 1940.

In general, a company which is or holds itself out as being engaged primarily in the business of investing, reinvesting or trading in securities, may be deemed to be an investment company under the U.S. Investment Company Act of 1940. We do not believe that we are an investment company as defined under the U.S. Investment Company Act of 1940. However, if we were to be deemed an investment company, we would be prohibited from issuing our securities in the United States and may have to terminate our U.S. listing or other sponsorship promoting a U.S. trading market for our issued securities. In order to avoid these prohibitions, we may be forced to forego otherwise attractive business opportunities, potentially limiting our growth and our profitability.

BECAUSE OF THE INFLUENCE OF OUR PRINCIPAL SHAREHOLDERS, OUR OTHER SHAREHOLDERS MAY BE UNABLE TO INFLUENCE OUR BUSINESS.

Our principal shareholders, including major shareholders who beneficially own more than 5% of the issued shares of our common stock and directors, beneficially owned approximately 34.4% of our outstanding shares as of December 31, 2005. These shareholders, if they act together, would be able to significantly influence all matters requiring approval by our shareholders, including the election of directors and the approval of mergers or other business combination transactions. Our principal shareholders may have strategic or other interests that conflict with the interests of our other shareholders. As a result, the concentration in our shareholdings may have the effect of delaying or preventing a change in control of Trend Micro, which could result in the loss of a significant financial gain to our shareholders.

OUR STOCK PRICE IS VOLATILE, AND INVESTORS BUYING THE SHARES OR ADSs MAY NOT BE ABLE TO RESELL THEM AT OR ABOVE THEIR PURCHASE PRICE.

Shares of our common stock are traded on the Tokyo Stock Exchange, which is the principal market for our shares. Recently, the U.S. and Japanese securities markets have experienced significant price and volume fluctuations. The market prices of securities of high-tech companies, and internet companies in particular, have been especially volatile. Since trading in our shares commenced on the Tokyo Stock Exchange on August 17, 2000, our stock price has fluctuated between a low of (Yen) 1,440 and a high of (Yen) 9,005. Since trading in our ADSs commenced on the Nasdaq National Market on July 8, 1999, the price of our ADSs has fluctuated between a low of $12.16 and a high of $159.38. The closing price on the Tokyo Stock Exchange for our stock on May 31, 2006 was (Yen)3,840, and the closing price on the Nasdaq National Market for our ADSs on May 31, 2006 was $35.00 per ADS. The market price of our shares and ADSs is likely to fluctuate in the future.

BECAUSE OF DAILY PRICE RANGE LIMITATIONS UNDER JAPANESE STOCK EXCHANGE RULES, YOU MAY NOT BE ABLE TO SELL YOUR SHARES OF OUR COMMON STOCK AT A PARTICULAR PRICE ON ANY PARTICULAR TRADING DAY, OR AT ALL.

Stock prices on Japanese stock exchanges are determined on a real-time basis by the equilibrium between bids and offers. These exchanges are order-driven markets without specialists or market makers to guide price formation. To prevent excessive volatility, these exchange set daily upward and downward price fluctuation limits for each stock, based on the previous day s closing price. Although transactions may continue at the upward or downward limit price if the limit price is reached on a particular trading day, no transactions may take place outside these limits. Consequently, an investor wishing to sell at a price above or below the relevant daily limit may not be able to sell his or her shares at such price on a particular trading day, or at all.

THE RIGHTS OF SMALL SHAREHOLDERS ARE LIMITED UNDER THE JAPANESE UNIT SHARE SYSTEM.

Our Articles of Incorporation provide that 500 shares of our common stock constitute one unit. The Japanese Company Law (as defined in Item 10.B) restricts the rights of shares that do not constitute whole units. Holders of shares constituting less than one unit do not have the right to vote. Each ADS offered in the offering represents the right to receive one share. A holder who owns less than 500 ADSs will indirectly own less than a whole unit. Under the deposit agreement governing the rights of ADS holders, in order to withdraw any shares, an ADS holder must surrender ADRs evidencing 500 ADSs or a multiple of 500 ADSs. Each ADR will bear a legend to that effect. Under the unit share system, holders of less than a unit have the right to require us to purchase their shares. Holders of ADSs that represent other than multiples of whole units cannot withdraw the underlying shares representing less than one unit. They will, therefore, be unable, as a practical matter, to:

exercise the right to require us to purchase the underlying shares, or

receive cash settlement in lieu of withdrawal.

As result, as a holder of ADSs, you will not be able to access the Japanese markets through the withdrawal mechanism to sell shares in lots of less than one unit.

AS A HOLDER OF ADSs, YOU WILL HAVE FEWER RIGHTS THAN A SHAREHOLDER HAS AND YOU WILL HAVE TO ACT THROUGH THE DEPOSITARY TO EXERCISE THOSE RIGHTS.

The rights of shareholders under Japanese law to take actions, including voting their shares, receiving dividends and distributions, bringing derivative actions, examining our accounting books and records and exercising appraisal rights are available only to holders of record. Because the depositary, through its custodian agents, is the record holder of the shares underlying the ADSs, only the depositary can exercise those rights in connection with the deposited shares. The depositary will make efforts to vote the shares underlying your ADSs as instructed by you and will pay you the dividends and distributions collected from us. However, in your capacity as an ADS holder, you will not be able to bring a derivative action, examine the accounting books and our records or exercise appraisal rights through the depositary.

RIGHTS OF SHAREHOLDERS UNDER JAPANESE LAW MAY BE MORE LIMITED THAN UNDER THE LAW OF OTHER JURISDICTIONS.

Our Articles of Incorporation, our Board of Directors regulations and the Japanese Company Law govern our corporate affairs. Legal principles relating to such matters as the validity of corporate procedures, directors and officers fiduciary duties and shareholders rights may be different from those that would apply if we were a non-Japanese company. For example, under the Japanese Company Law, only holders of 3% or more of the issued and outstanding shares are entitled to examine our accounting books and records. Shareholders rights under Japanese law may not be as extensive as shareholders rights under the laws of other countries. You may have more difficulty in asserting your rights as a shareholder than you would as a shareholder of a corporation organized in another jurisdiction. In addition, Japanese courts may not be willing to enforce liabilities against us in actions brought in Japan which are based upon the securities laws of the United States or any U.S. state.

Item 4. Information on the Company.

A. History and Development of the Company.

We develop, market and support antivirus and Internet content security software and services. Our legal name in Japan is Trend Micro Kabushiki Kaisha and Trend Micro Incorporated in the United States. Our commercial name in both Japan and the United States is Trend Micro. Founded in 1988 by Steve Chang, we led the migration of virus protection from the desktop to the network server and the Internet gateway. Today, through Trend Micro Enterprise Protection Strategy, we focus on providing customers with an approach to managing the impact of mixed threats such as the NIMDA and Code Red viruses.

We were established in 1989 as a Taiwanese company. Through a series of transactions in August 1996, Trend Micro Kabushiki Kaisha (a joint stock corporation) which was established in October 1988, became the parent company of the Trend Micro group.

Our head office is located at Shinjuku MAYNDS Tower, 1-1, Yoyogi 2-Chome, Shibuya-ku, Tokyo 151-0053, Japan. Our telephone number is 81-3-5334-3600. Our North American headquarter is in Cupertino, California, U.S.A. and we have business units worldwide. We have no agent in the United States in connection with this annual report.

We began commercial operations in May 1989, shortly after computer viruses were first detected, and we completed our initial public offering on the Japanese over-the-counter market in August 1998. We listed American Depositary Shares on the Nasdaq National Market in July 1999 in connection with a global offering of 12,750,000 shares in the form of shares and ADRs. In August 2000, we listed on the first section of Tokyo Stock Exchange.

We currently have more than 2,900 employees and are represented more than 30 countries.

B. Business Overview.

INDUSTRY BACKGROUND

A computer virus is a program a piece of executable code that has the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. With email now used as an essential business communication tool, viruses are spreading faster than ever. Viruses attached to email messages can infect an entire enterprise in a matter of minutes, which may cost companies millions of dollars annually in lost productivity and clean-up expenses. Mixed-threat attacks like NIMDA and MSBlast, threaten computer systems at multiple levels.

Today the threats on the network such as computer viruses, spyware, spam and phishing are not the nature that can be predicted beforehand and treated with all possible measures. It seems there is now a requirement for enterprises and individuals to deploy security measures against new network threats and crimes which can cause monetary damages and disable networks around the world.

To enhance our capability against new threats evolving day by day, we acquired InterMute Inc. which provides anti-spyware technologies and Kelkea Inc. which provides IP filtering and reputation services in 2005.

In response to the virus threat above, the antivirus software market has grown significantly in the past few years and expected to continue to grow in the future.

According to International Data Corporation, an independent research organization, in December 2005, the anti-virus industry, which we belong to, will increase from $3.7 billion in 2004 to $7.3 billion in 2009 and is estimated to expand at a compound annual growth rate of around 15% from 2005 to 2009.

Our vision is to create A world safe for exchanging digital information . We offer solutions to prevent the invasion of viruses and other malicious content into corporate networks, small and medium business networks and individual PCs.

Network systems including the Internet are an integral part of corporate activities and life at home. However, the methods viruses use to access computers have become more elaborate and malicious, causing serious problems for users. Furthermore, problems are arising where spyware, spam and inappropriate Web use diminish the functionality and efficiency of network and Internet use.

Against this backdrop, the needs of corporate networks and individual users for security vendors have expanded and intensified. Our role extends beyond merely developing and selling security products. We also provide services to offer a more effective security solution. Through this business model, we are contributing to the development of a safe digital society around the world.

Our products and services have evolved with the development of the antivirus software market. Initially, our sales of antivirus software products consisted primarily of sales of our desktop programs, such as PC-cillin/Virus Buster, which were introduced in Japan in 1991. To meet increased demand for network-based products as companies shifted from stand-alone desktop PCs to client-server enterprise networks in the early 1990s, we introduced LANprotect, our first server application, in 1993. To address the increased risk of virus infection for enterprise networks resulting from widespread use of the Internet, we introduced InterScan VirusWall in 1996 to provide real-time scanning at the Internet gateway, the point where data enters the network from the Internet. In 1998, we introduced Trend Virus Control System, the forerunner of Trend Micro Control Manager (described below), which enabled network-wide antivirus software to monitor, update and manage from a central management console. Since 1998 we have continued to develop our Internet security solutions, and in 2002 we unveiled Trend Micro Enterprise Protection Strategy, which is described below.

Trend Micro Enterprise Protection Strategy

Trend Micro Enterprise Protection Strategy, our threat and outbreak management strategy to prevent computer viruses, is implemented using centralized management of an integrated security suite and outbreak prevention appliance. This solution is supported by real-time, threat-specific knowledge from TrendLabs, Trend Micro s global network of security experts.

We help and enable IT managers to proactively manage the outbreak lifecycle. This lifecycle consists of four phases vulnerability prevention, outbreak prevention, virus response and assessment and restoration.

Vulnerability Prevention

In this phase, vulnerability assessment tools help enforce security policies, block noncompliant devices from network access and isolate specific threat-related vulnerabilities to pre-empt attacks. Trend Micro Vulnerability Assessment is a key product component of this phase. Centrally managed by Trend Micro Control Manager, a centralized outbreak management console, Vulnerability Assessment integrates with other Trend Micro products and services to identify vulnerabilities in the network. Vulnerability Assessment determines risk ratings to alert IT managers of specific viruses correlated with system vulnerabilities and identifies patches needed to prevent exploits. Leveraging data from Vulnerability Assessment, Trend Micro Network VirusWall (described below) assists IT managers to selectively perform the following actions:

- Isolate unpatched machines for Microsoft operating system vulnerabilities before or at the onset of an outbreak.
- Quarantine infected LAN segments to stop virus propagation.
- Check devices for the latest pattern files, scan engine, and antivirus software from major antivirus vendors, to control network access of noncompliant machines.

Outbreak Prevention

The outbreak prevention phase is the critical period when a threat has been identified, but a pattern file or patch has not yet been deployed. Without sufficient information, IT managers struggle not only to identify protective actions but also to deploy them effectively across the organization. Trend Micro Outbreak Prevention Services include outbreak prevention policies, which are strategic recommendations to manage the various methods in attacking viruses and to assist IT managers in deflecting, isolating, and stopping virus outbreaks. Through Trend Micro Control Manager, outbreak prevention policies can be deployed manually or automatically to block any combination of file extensions, executables, IP addresses, ports, instant message channels, and file transfer protocols. IT managers can use outbreak prevention policies to perform the following actions:

- Keep viruses from propagating and impeding network traffic;
- Automatically activate Trend Micro Damage Cleanup Services (described below) to ease administrative burden; and
- Generate detailed reports for threat analyses.

Virus Response

The virus response phase of the outbreak lifecycle occurs during the deployment of a pattern file, network signature, or patch. This reactive phase is the single focus of most antivirus products. In contrast, Trend Micro Control Manager coordinates virus response with outbreak prevention policies to enable proactive outbreak lifecycle management from a central console. Our scanning engines provide IT managers with the following benefits:

Comprehensive protection with virus scanning and detection at both the network layer and the application layer;

Increased accuracy, scanning performance and virus detection with scanning engines that search for viruses based on the identified threat; and

A guarantee (Trend Micro Service Level Agreement) that new virus pattern files will be delivered within two hours of virus case submission or Trend Micro will pay a certain penalty fee depending on the terms of the agreement entered into with the customer.

Assessment and Restoration

The assessment and restoration phase of the outbreak management lifecycle is the period after a pattern file, network signature, or patch is deployed and the virus has been contained. Cleaning the network of virus remnants and restoring systems is tedious and costly because most organizations perform these tasks manually. In contrast, Trend Micro Damage Cleanup Services automate clean-up and restoration to mitigate administrative cost and burden. Centrally managed through Trend Micro Control Manager, Damage Cleanup Services feature agent-less remote deployment, allowing IT managers to assess, clean, and restore infected PCs and servers located in remote locations without end-user intervention. Damage Cleanup Services are designed to result in cost-effective clean-up by helping IT managers do the following:

Prevent re-infection by removing memory resident worms and Trojans (a type of virus that can conceal itself) and their effects, such as unwanted registry entries and viral files;

Reduce administrative burden via coordination with outbreak prevention policies; and

Perform consistent clean up aided by detailed reports from Trend Micro Control Manager.

Distribution of a Defective Virus Pattern File in April 2005

On April 23,2005, Trend Micro published pattern file 2.594.00 with the intent to protect customers from a new type of BOT virus that could cause an infected PC to become a launching point for spam. Given the number of variants of this threat and what they are designed to do, we believe they have the potential to cause great damage to users and puts at risk the safety and integrity of the networks through which they might spread. Unfortunately, pattern file 2.594.00, which employed a new, generic unpacking and heuristic script technology designed to detect and eliminate these new types of BOT viruses and their variants, generated some performance conflict with computers running on Microsoft Windows XP and certain other operating systems. As a result, this caused the impacted machines to experience high CPU consumption and subsequent system instability.

For any customers experiencing instability, Trend Micro has provided a set of solutions which can be found under the Support section of Trend Micro s website. Additionally, Trend Micro has extended support hours especially to help those customers who had this special intersection of circumstances and were affected by this issue. Trend Micro continued testing in order to fully understand initial assessments and fix the issue. We found that the pattern file caused performance issues on systems with Scan Engine 7.5 and above while scanning a particular type of executable file found in certain versions of operating system service packs. Owing to a large number of variants discovered by our researchers of a particular BOT threat (each of which used a different compression algorithm), Trend Micro enhanced the decompression ability of its pattern file with a view to prevent further variants of this BOT from infecting customers. However, within pattern file 2.594.00, TrendLabs included support for 3 additional heuristic patterns, including UltraProtect decompression support, which is used by several WORM_RBOT variants. Due to an isolated anomaly in the engineering, development and pattern release process, the UltraProtect decompression may in certain circumstances cause some systems to experience high CPU power consumption, which can lead to system instability when this specific file type is scanned using pattern file 2.594.00.

Through its analysis, Trend Micro has determined that while pattern file 2.594.00 was designed to prevent several new variants of a fairly new type of BOT threat from infecting its customers, the issues with pattern file 2.594.00 were caused by how the testing was conducted for this type of solution. Therefore, we are taking the following steps to ensure that future instances of this issue do not occur.

We have invested in additional resources to immediately improve our development, review, testing and monitoring processes to ensure efficient execution of Trend Micro virus pattern signatures.

We are developing an automated method within the tool used to create virus pattern signatures. This automation would help to determine the potential for possible future instances of high CPU utilization caused by our pattern files.

We are enhancing the Scan Engine to include a self-monitoring mechanism.

We are increasing the scope and support of our testing coverage and of our processes to prevent reoccurrence of such issues.

Trend Micro Products and Services

Our products and services are designed to deliver coordinated protection at the file, application, data, and network layers to proactively manage the outbreak lifecycle. Our solutions, described in more detail below, operate across a range of computer operating system platforms, including Windows Server 2003, Windows NT, Windows 98/XP/2000, Linux, Sun Solaris and several versions of UNIX. Our products protect all entry points in the network.

Management Products

Control Manager

Trend Micro Control Manager is a centralized outbreak management console designed to simplify enterprise-wide coordination of outbreak security actions and management of Trend Micro products and services. Trend Micro Control Manager acts as a central command center for deployment of Trend Micro s threat-specific expertise across the network and to select third-party products to proactively manage outbreaks.

Designed to deliver the flexibility and scalability organizations need, Trend Micro Control Manager offers a multi-tier management structure with extensive customization options for expanded control. Robust graphical reporting provides vital security insights such as sources of infections or vulnerabilities and consolidated, detailed information regarding virus events or unusual activities

Network VirusWall 2500

Network VirusWall 2500 delivers security unmatched by any other appliance vendor. It stops network worms and vulnerability exploits with complete accuracy. To prevent infection, it enforces security policies by blocking noncompliant devices from network access (for remediation). It isolates infected network segments and automates remote clean up in case of outbreak.

Network VirusWall 2500 is deployed inline with network traffic to address the threat to network security from network worms. It protects up to 4096 concurrent users with a 10/100/1000 Gigabit Ethernet copper + fiber interface and features flexible configurations for high availability and redundancy to protect enterprises and mission-critical applications from attack. Four additional ports allow Network VirusWall 2500 to protect multiple network segments or servers.

Network VirusWall 1200

Network VirusWall 1200 delivers security unmatched by any other appliance vendor. It stops network worms and vulnerability exploits with complete accuracy. To prevent infection, it enforces security policies by blocking noncompliant devices from network access (for remediation). It also isolates infected network segments and automates remote clean up in case of outbreak.

Network VirusWall 1200 is deployed inline with network traffic at a local area network (LAN) or virtual private network (VPN) segment to addresses the threat to network security from worms. It features a 10/100 Base-T Ethernet interface to protect up to 256 users with two ports and one inline segment.

Network VirusWall 300

Trend Micro Network VirusWall 300 Outbreak Prevention Appliance for Mission-Critical Devices Security products such as desktop or host-based antivirus, firewalls, and intrusion detection systems cannot effectively stop network worms from propagating to remote devices. Network worms can degrade network performance and take mission critical devices offline.

Trend Micro Network VirusWall 300 is an outbreak prevention appliance designed to protect mission-critical devices (examples: ATMs, self-service kiosks, medical devices, etc.) from network worms and to clean up infections to keep worms from spreading. Because there are no hardware or software compatibility issues with the appliance, enterprises can deploy Network VirusWall 300 to protect any IP-enabled device.

Unlike security solutions that monitor threats or provide threat information only, Network VirusWall 300 deploys threat-specific knowledge from TrendLabs(SM) at network end points to help organizations prevent or mitigate damage from worms. Network VirusWall appliances help organizations improve their operational resilience by lowering security risks, easing the virus outbreak management burden, and reducing system downtime.

Internet Gateway Products

Spam Prevention Solution seamlessly integrates with InterScan Messaging Security Suite to combine high-performance spam protection with leading antivirus and content filtering all in a single platform at the Internet messaging gateway. The anti-spam module features a powerful new composite engine that blends advanced heuristics, signature filters, blacklists/whitelists, and improved multi-lingual detection a breakthrough for blocking spam and phishing attacks at higher catch rates and with fewer false positives.

To enhance our capability of anti-spam, we acquired Kelkea, Inc. which provides IP filtering and reputation services.

InterScan Messaging Security Suite

InterScan Messaging Security Suite integrates high-performance antivirus and content filtering security plus the optional Trend Micro Spam Prevention Solution with anti-spam and anti-phishing all in a single platform at the Internet messaging gateway. As an integrated solution, it filters SMTP and POP3 traffic to stop viruses, spam, phishing, and mixed threat attacks at the network s most critical point of entry. A centralized management console enables administrators to set coordinated policy, automate updates, and control message compliance for a more effective, unified defense.

InterScan Web Security Suite

Trend Micro InterScan Web Security Suite provides the first line of defense against multiple Web-based threats blocking attacks at the gateway. It guards against viruses, spyware, grayware, and phishing, and offers optional security modules to combat malicious mobile code and manage employee Internet use. The suite integrates with optional Trend Micro Damage Cleanup Services to remove threats and restore infected files. As a fully integrated solution, it is easy to deploy, manage, and maintain lowering the total cost of ownership.

InterScan VirusWall

InterScan VirusWall provides high-performance, comprehensive Internet gateway protection against viruses and malicious code. The optional eManager plug-in offers administrators additional tools for spam blocking, content filtering, and email scheduling.

InterScan eManager

InterScan eManager provides real-time content filtering, spam blocking, and reporting to help companies monitor and control the type of information that enters or leaves the network. The optional eManager plug-in integrates seamlessly with InterScan VirusWall to safeguard intellectual property and confidential information, block inappropriate email and attachments, and protect against viruses. eManager also enables Trend Micro Outbreak Prevention Services to provide proactive protection against virus outbreaks by deploying attack-specific policies to contain the outbreak.

InterScan AppletTrap

InterScan AppletTrap protects against known and unknown malicious applets, ActiveX, JavaScript, and VBScript code at the Internet gateway. AppletTrap features patented technologies including Java instrumentation to monitor applet behavior in real time. Its patented, multi-tiered process safeguards enterprise computing environments through analysis and verification of digital certificates, filtering for known malicious code, and monitoring the behavior of unsigned code at the client browser to help protect against unknown malicious applets. A centrally managed policy-based management tool, AppletTrap requires no client deployment and is transparent to end users.

InterScan WebProtect for ISA

Easy to handle, integrated, industry-leading antivirus solution for Microsoft ISA Servers.

InterScan Antivirus for Sendmail

Trend Micro InterScan Antivirus for Sendmail delivers scalable, high-performance protection against viruses and other forms of malicious code that enter SMTP traffic. This targeted solution enables Sendmail Switch Edition customers to benefit from the leading Internet gateway virus security #1 for five years in a row, according to an IDC analyst report. The security application can be centrally managed through Sendmail s unique console, providing a familiar interface for administrators to adjust and enforce security policies for all PCs across the enterprise.

Network Reputation Services

As the first line of defense, Trend Micro Network Reputation Services stop up to 80% of spam at its source before it can flood your network, overload mail gateway security, and burden IT resources. To block spam, the IP address of incoming mail is verified against one of the world s largest and trustworthy reputation database of known spam sources. Plus, Dynamic Real-Time Spam Blocking identifies new sources of spam, even zombies and botnets, as soon as they begin spamming.

Network Reputation Services integrate with Trend Micro s messaging gateway security solution InterScan Messaging Security Suite and Spam Prevention Solution for a 3-in-1 defense against viruses, spam, phishing, and mixed threat attacks. By reducing spam s impact on the gateway, reputation services allow messaging security to run at optimal efficiency.

Email, Messaging & Groupware Products

ScanMail for Microsoft Exchange

Trend Micro ScanMail for Microsoft Exchange guards against viruses, Trojans, worms, and other malicious code hidden in email attachments. By filtering inbound/outbound SMTP connector-level traffic, it blocks threats before they can enter or leave the mail server. For additional security, Trend Micro ScanMail Suite for Microsoft Exchange combines virus protection with new anti-spam and advanced content filtering technology. A centralized management console makes it easy to deploy group configurations, scan settings, notifications, and automatic updates across all Exchange servers.

ScanMail eManager

ScanMail eManager provides real-time content filtering, spam blocking, and reporting to help companies monitor and control the type of information that enters or leaves the network. The optional eManager plug-in integrates seamlessly with ScanMail for Microsoft Exchange and ScanMail for Lotus Notes to safeguard intellectual property and confidential information, block inappropriate email and attachments, and protect against viruses. eManager also enables Trend Micro Outbreak Prevention Services to provide proactive protection against virus outbreaks by deploying attack-specific policies to contain the outbreak.

ScanMail for Lotus Domino

ScanMail for Lotus Domino 3.0 offers comprehensive virus protection and content security for Lotus Domino/Notes environments. It scans email in real time for viruses and spyware hidden within email attachments and databases. Unlike many other security products, ScanMail for Lotus Domino was specifically designed for use as a Lotus Domino server application and is optimized for high-performance scanning.

ScanMail Suite for Lotus Domino 3.0 also provides anti-spam and systematic content filtering for an additional layer of protection. Both solutions currently support Microsoft Windows , Sun Solaris , Linux on x86, IBM AIX , and i5/OS // OS/400 .

Trend Micro IM Security for Microsoft Office Live Communications Server

Trend Micro IM Security for Microsoft Office Live Communications Server (LCS) delivers advanced protection from malicious code and inappropriate content. IM Security can be centrally managed and administered, and runs with minimal performance impact to LCS. Incident-based archives support quick and easy searches for content violations. Complete with instant notification through LCS and comprehensive real-time reporting, IM Security helps administrators deploy and maintain a virus-free IM environment with secure content.

File Server & Storage Products

ServerProtect for Microsoft Windows/Novell NetWare

ServerProtect provides comprehensive antivirus scanning for servers, detecting and removing viruses from files and compressed files in real time before they reach the end user. Administrators can use a Windows-based console for centralized management of virus outbreaks, virus scanning, virus pattern file updates, notifications, and remote installation. ServerProtect supports Microsoft Windows Server 2003, Microsoft Windows 2000, Microsoft Windows NT 4, and Novell NetWare servers.

ServerProtect for Network Appliance filers

ServerProtect provides antivirus scanning for Network Appliance filers, detecting and removing viruses from files and compressed files in real time - before they reach the end user. Administrators can use a Windows-based console for centralized management of virus outbreaks, virus scanning, virus pattern file updates, notifications, and remote installation.

ServerProtect for EMC Celerra

ServerProtect provides antivirus scanning for EMC Celerra file servers, detecting and removing viruses from files and compressed files in real time - before they reach the end user. Administrators can use a Windows-based console for centralized management of virus outbreaks, virus scanning, virus pattern file updates, notifications, and remote installation.

ServerProtect for Linux

Trend Micro ServerProtect for Linux provides comprehensive real-time protection and cleaning against computer viruses, Trojans, and worms for Linux servers and desktops. Managed through an intuitive, Web-based management console - now with Mozilla support - ServerProtect allows centralized virus scanning, pattern updates and event reporting. ServerProtect can easily manage virus maintenance tasks such as initiating on-demand scanning, printing/exporting/purging virus logs and setting parameters for real-time scanning.

PortalProtect for SharePoint

Trend Micro PortalProtect provides comprehensive virus protection and content filtering for Microsoft SharePoint Portal Server 2003 and Windows SharePoint Services. Real-time, scheduled, and manual scans prevent viruses, Trojans, worms, and other malicious code from entering or residing in the portal, while content filtering blocks potential threats and unwanted content. It is built on Trend Micro s award-winning scan engine and tightly integrates with the Microsoft antivirus API for optimal security and high-speed performance with minimal impact on system resources.

A Web-based management console offers secure, convenient access to management tools, including customized reports and activity logs. Plus, it automatically deploys scan engine and pattern file updates for protection from the latest threats.

Trend Micro Housecall Server Edition

Trend Micro HouseCall Server Edition is a browser-based application that allows users to quickly scan and clean their PCs of malware before they access the network. Strategically placed at user access points, HouseCall Server Edition acts as a checkpoint station to protect network resources from viruses and spyware that enter when users access the network with infected machines. It lowers the risk of infection while providing users with a valuable service. HouseCall Server Edition helps organizations reduce help desk and support costs, protect sensitive data, and maintain customers trust. The Web-based service is easy to deploy and use, avoiding high implementation and user training costs. Deployed on an intranet or extranet server, HouseCall Server Edition complements antivirus and anti-spyware solutions from major security vendors.

Desktop Products

OfficeScan

Trend Micro OfficeScan Client/Server Edition protects enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks. As an integrated solution, it guards desktops, laptops, and network servers, while the Web-based management console makes it easy to set coordinated security policy and deploy automatic updates on every client and server. By integrating with Trend Micro Network VirusWall or any Network Admission Control (NAC) device, OfficeScan can enforce policy on non-compliant computers, and then remedy, redirect, restrict, deny, or permit network access.

Trend Micro Anti-Spyware Enterprise Edition

Trend Micro Anti-Spyware Enterprise Edition is a standalone anti-spyware solution that protects clients and servers with superior spyware detection and cleanup supported by true enterprise-class management. It stops spyware from installing by actively monitoring file downloads. A highly efficient spyware database and heuristic rule set scan and clean clients accurately, with a small footprint. It is the only product that includes Trend Micro CWShredder to eradicate CoolWebSearch browser hijackers. Centralized management eases administration and deployment while supporting large organizations needs for scalability at multiple levels. Anti-Spyware Enterprise Edition is compatible with major enterprise desktop security products.

PC-cillin Internet Security

Trend Micro PC-cillin Internet Security 2006 combines award-winning antivirus security and a personal firewall for comprehensive protection against viruses, worms, Trojans, and hackers. It also detects and removes spyware and blocks spam. It even guards against identity theft by blocking phishing and pharming attacks. Plus, PC-cillin protects wireless network with Wi-Fi Intrusion Detection, an innovative security feature that alerts users when an intruder uses Wi-Fi connection.

Trend Micro Anti-Spyware

Trend Micro Anti-Spyware is a comprehensive spyware detection and removal solution, designed especially for home users. Built on technology that has shipped on more new PCs from major computer manufacturers than any other anti-spyware product available, it features solid detection capabilities to help identify and halt attacks before they can cause unrecoverable damage. Unlike other spyware products, Trend Micro Anti-Spyware features thorough cleaning technology to help ensure proper removal of unwanted spyware remnants.

To enhance our capability of anti-spyware, we acquired InterMute, Inc. which provides anti-spyware technologies.

Trend Micro Home Network Security

Trend Micro Home Network Security combines Internet security technology built into select models of home routers with award-winning Internet security on each PC. As an integrated hardware/software solution, it provides seamless, easy-to-use protection for your entire home network. A single, convenient subscription guards against viruses, hackers, spyware, spam, and mixed threat attacks. Plus, router-based Parental Controls make it easy to manage your children s Web surfing activities without having to install software on each PC.

Mobile Security Products

Trend Micro Mobile Security

As the number of data-centric mobile devices grows, industry analysts expect them to become the next target of virus writers. Users can protect their smartphone or wireless handheld against these threats with Trend Micro Mobile Security. Trend Micro Mobile Security helps protect data-centric mobile devices from the evolving threats of viruses and SMS text message spam. The mobile security solution enables mobile operators to maximize airtime, revenues, and customer satisfaction and minimize the customer service calls and churn resulting from virus infections. Enterprises can use Trend Micro Mobile Security to mitigate virus threats from handheld devices and ensure mobile-user productivity.

Small and Medium Business Products

Trend Micro Security Solutions save time, effort and money for SMBs with limited IT resources. They are easy to deploy, effortless to maintain and offer comprehensive protection.

Trend Micro Anti-Spyware for SMB

Trend Micro Anti-Spyware for Small and Medium Businesses (SMBs) is the valuable standalone anti-spyware solution that automatically delivers best-in-class spyware detection and removal capabilities to networked PCs and servers. Using real-time protection to help stop spyware from operating, installing, or downloading to PCs and servers, Trend Micro Anti-Spyware for SMB helps prevent information leakage and enhances privacy protection.

The proven solution shares the same trusted technology that has been preinstalled on over 6 million PCs by major computer manufacturers. With its silent deployment, automatic updates, and remote management capabilities, Trend Micro Anti-Spyware for SMB provides worry-free spyware protection that busy IT managers can set and forget.

Client Server Security for SMB

Trend Micro Client Server Security for SMB protects PCs and Windows servers, against viruses and hackers in an all-in-one integrated defense. It dramatically simplifies security management for businesses who demand a worry-free approach. Automatic Threat Protection eliminates the time and costs of manually dealing with viruses, worms, and other malicious code. It s like having a virtual 24/7 security staff. In addition, the complexity and the effort necessary to protect your business from multiple Internet threats are reduced by an all-in-one Integrated Defense. Finally, Zero Administration relieves users of managing security solutions so they can stay focused on their business.

Client Server Messaging Security for SMB

Trend Micro Client Server Messaging Security for Small and Medium Business protects PCs, Windows servers, and Microsoft Exchange servers against viruses, spam and hackers in an all-in-one integrated defense. Trend Micro Client Server Messaging Security for SMB dramatically simplifies security management for businesses who demand a worry-free approach.

For example, Automatic Threat Protection eliminates the time and costs of manually dealing with viruses, spam and other malicious code. It is like having a virtual 24/7 security staff. In addition, the complexity and the effort necessary to protect your business from multiple Internet threats are reduced by an all-in-one Integrated Defense. Finally, Zero Administration relieves users of managing security solutions so they can stay focused on their business.

InterScan VirusWall for SMB

Trend Micro InterScan VirusWall for Small and Medium Business, the most comprehensive gateway antivirus, anti-spam and content filtering solution of its kind, protects against malicious threats at the gateway before they reach the interior of your network. Designed for growing companies, it filters Internet email and Web traffic to ensure that content is free of viruses and spam. While most of competing products need to be managed separately, InterScan VirusWall for Small and Medium Business features a single point of management with an intuitive interface that facilitates administration and lowers the total lifetime cost of your security strategy.

InterScan VirusWall for Small and Medium Business provides a high degree of protection at the gateway, featuring in-depth scans of SMTP, HTTP, and FTP streams. Furthermore, it also checks POP3 traffic helping to ensure that networks are protected even when employees access their Internet email accounts. Integrated anti-spam and email content filtering also help maintain productivity and ensure the appropriate use of Internet resources.

NeatSuite for SMB

NeatSuite for Small and Medium Businesses, a comprehensive security suite, delivers enterprise-caliber antivirus, content security and anti-spam technologies in a single purpose-built package. This powerful solution set empowers business owners to deploy and manage an effective end-to-end antivirus and anti-spam strategy with limited IT investment. NeatSuite for Small and Medium Businesses minimizes the Internet threats that can infiltrate via open communication channels necessary to do business Email (SMTP, POP3), Web access (HTTP), and File download (FTP). Leveraging Trend Micro s industry-pioneering technology, NeatSuite for Small and Medium Businesses offers complete gateway, e-mail, server and PC protection in one, easy to manage package. Its single point of management and intuitive interface facilitates easy installation, configuration, and administration thus reducing the total cost of ownership.

Services and Support

We provide several industry-unique services that complement our products, including information deployment and attack-specific policies and cleaning templates that help minimize the impact of network viruses, network vulnerabilities, and mixed-threat attacks. We offer a range of services, backed by timely knowledge and expertise from TrendLabs, including Trend Micro Vulnerability Assessment, Trend Micro Outbreak Prevention Services, Virus Response Services, and Trend Micro Damage Cleanup Services, to help customers manage all phases of the virus outbreak lifecycle.

Virus Response Service Level Agreement guarantees customers that fully tested virus pattern files will be delivered within two hours from the time a virus case is submitted. If we fail, however, based on the terms of the agreement entered into with the customer, we may make a penalty payment which may amount up to 100% of the initial sale price.

Premium Support Program provides customers with timely assistance that combines rapid response times with technical and computer security expertise to quickly address customer issues. A wide range of service plan options are offered that provide varying levels of personalized customer service from enhanced online support to dedicated on-site support.

Our products are backed by TrendLabs, a global network of antivirus research and support centers with an ISO9001:2000 and BS7799. Staffs in a head center of TrendLabs are more than 700 including engineers and antivirus specialists operate around the clock to monitor virus activity, develop information on new threats, and deliver prompt, effective services designed to deal with specific threats.

Seasonality

Our quarterly net sales are subject to seasonal fluctuations. For example, net sales of corporate products in Japan may be lower in the quarters ending June and December, and higher in the quarters ending March and September, while net sales of consumer products in Japan may be higher in the quarter ending December. Net sales of corporate products in the United States and Europe may be lower in the quarter ending March and higher in the quarter ending December.

SALES AND MARKETING

Our products are generally sold to corporate customers on a per-user license basis through our channel partners which include systems integrators, distributors, and value-added resellers, with the remaining portion consisting largely of package software sales through channel partners and our online Web stores. We view our channel partnerships as key to our success. Our support programs, such as training and certification programs for our products, help cultivate relationships with our channel partners. Channel partners are integral to increasing the brand recognition and visibility of Trend Micro products and services in the network antivirus and Internet content security market.

In our marketing strategy, Trend Micro Enterprise Protection Strategy plays a central role. By emphasizing this industry-unique approach through media and industry analyst community, interest for Trend Micro products and services is generated at the customer level primarily through our channel partners as well as through our global Web sites, corporate alliances, advertising in trade and business publications, customer references, direct marketing campaigns, and trade shows and events worldwide. Furthermore, an extensive and expertise-driven service and support organization contribute to customer loyalty. Current marketing efforts are targeted at a combination of large enterprise, small and medium businesses, as well as consumer and broadband customers.

Regional Overview

Japan

Overview. We sell our products in Japan to both corporate and individual end users primarily through systems integrators and distributors, and conduct a limited amount of direct sales to end users, including online sales through a reseller s website. Our net sales in Japan accounted for approximately 40% of our net sales or (Yen)29.4 billion in 2005, approximately 41% of our net sales or (Yen)25.4 billion in 2004 and approximately 42% or (Yen)20.1 billion in 2003.

Distribution Through Systems Integrators and Distributors. Virtually all sales to Japanese corporate users are made through systems integrators. In Japan, systems integrators play a large role in delivering management information services, providing primary computer support services such as installation, systems integration, upgrades, and maintenance.

Relationship with SOFTBANK. Since 1996, we have entered into numerous agreements with SOFTBANK in connection with the distribution of our products in Japan by SOFTBANK. Currently, all distribution by SOFTBANK of our products in Japan is covered by an October 1999 distribution agreement with SOFTBANK BB, an indirect wholly-owned subsidiary of SOFTBANK. This distribution agreement gives SOFTBANK BB the non-exclusive right in Japan to distribute all of our products. It is automatically renewable for successive one-year terms, unless either party exercises its right of non-renewal by giving prior written notice. The October 1999 distribution agreement supersedes all prior agreements between SOFTBANK and us relating to distribution of our products. We make rebate payments to SOFTBANK based on SOFTBANK s achievement of sales targets agreed upon between SOFTBANK and us.

Historically, a significant percentage of our Japan net sales have been sales to SOFTBANK. For example, sales to SOFTBANK BB totaled approximately (Yen)9.2 billion or 19.1% of net sales in 2003, (Yen)10.4 billion or 16.8% of net sales in 2004 and (Yen)10.6 billion or 14.5% of net sales in 2005. The majority of sales to SOFTBANK BB in 2003, 2004 and 2005 consisted of SOFTBANK BB s sales of our products to systems integrators.

Service Provider and Other Relationships. We contracted with Nifty, NTT-Communications, and Internet Initiative Japan to license InterScan VirusWall technology to them which enables them to provide virus scanning service to their subscribers. We entered into agreements with SECOM Trust net, Hitachi Software Engineering and Otsuka Shokai which allow them to provide antivirus outsourcing service to their customers.

North America

Overview. Our North American region includes the United States and Canada, with headquarters in Cupertino, California. Products are sold through distributors, value-added resellers and managed service providers. Our North America net sales accounted for approximately 21% of our net sales or (Yen)15.4 billion in 2005, approximately 19% of our net sales or (Yen)11.9 billion in 2004 and approximately 20% or (Yen)9.6 billion in 2003.

Distributors. The majority of our North American revenue is from sales of site licenses to corporate users and consumer products to home users. Principal distributors in the U.S. include Ingram Micro, Interwork Technologies, Navarre, Synnex and Techdata. In Canada, principal distributors include Interwork Technologies Canada, Ingram Micro Canada, Synnex Canada, and Tech Data Canada.

Our customers in the United States include the U.S. federal and state government agencies, educational institutions, large corporations from all industries, and small and medium sized businesses. A majority of the contracts were comprised of Internet gateway, e-mail and groupware products and client server products as described above.

Europe, the Middle East and Africa

Overview. We are represented throughout Europe, the Middle East and Africa (EMEA), with offices in Germany, France, Italy, Spain, U.K., Norway, Sweden, the Netherlands, Belgium, Poland and United Arab Emirates. Our European Support Center, which is located in Munich, Germany and Cork, Ireland, offers real-time technical support and antivirus expertise to our channel partners throughout Europe. Our EMEA net sales accounted for approximately 25% of our net sales or (Yen)18.4 billion in 2005, approximately 26% of our net sales or (Yen)16.4 billion in 2004 and approximately 25% or (Yen)12.1 billion in 2003.

Distributors. The majority of European revenues are from sales of site licenses to corporate users. Principal distributors for the EMEA region include: Belgium/Luxembourg/ Netherlands: NOXS, Intechnology Plc, Logix Plc and Tech Data. Middle East/Africa: SecureData, Online Distribution and Hilan Tech. France: Cris Reseaux, IP Vista, Noxs France, ComputerLinks, Avanquest France, InfoManage (Switzerland) and Config (North Africa). Germany: ComputerLinks AG, Entrada Kommunikations GmbH, Client Server EDV und Elektronic GmBH, Ingram Micro Distribution GmbH and Tech Data Midrange GmbH. Italy: IT Way SPA, ComputerLinks, Esprinet SPA and J.Soft Distribuzione SPA. Nordic Region: Network Technologies A/S (Denmark), Securesoft AB (Sweden), Scribona AS (Norway), Scribona Nordic AB (Sweden), Itegra AS (Norway), Securesoft Norway (AS) and Securesoft OY (Finland). Spain: AFINA, Itway Iberica SL and Diode. UK: e92plus Ltd, Sphinx and Unipalm.

Our customers in EMEA include various government departments, educational institutions, large corporations and small and medium sized businesses. A majority of the contracts include Internet gateway, email server, and client server products as described above.

Asia Pacific

Overview. We are represented throughout the Asia Pacific region (excluding Japan), with offices in Taiwan, Hong Kong, China, Singapore, Malaysia, Thailand, Indonesia, India, Korea, Australia, and New Zealand. Trend Micro s ISO9001:2000 and BS7799 standards-certified headquarters for TrendLabs, our global product support and antivirus research center, is located in Manila, the Philippines; this facility and others like it provide continuous 24 hours-a-day, seven-days-a week coverage to our customers around the world. Our Asia Pacific net sales accounted for approximately 11% of our net sales or (Yen)7.9 billion in 2005, approximately 10% of our net sales or (Yen)6.3 billion in 2004 and approximately 10% or (Yen)4.8 billion in 2003.

Distributors. The majority of Asia Pacific revenue is from sales of site licenses to corporate users and consumer products to home users. Principal distributors in Asia Pacific include: Taiwan: TWP, UCOM and Jetwell Computer. Hong Kong: Datalink, SIS, and Digital China. China: Digital China, Dawncom Business Technology and Service and Secure China Global Communication. South Asia: Ingram Micro, ACA Pacific, ECS Computer, Select Technologies. Korea: Daou System, Intercom Software and Sun Tek. Australia: Alstom IT, Ingram Micro, and Channelworx. New Zealand: Lan One and Soft Solutions.

Our customers in Asia Pacific include local government departments and agencies and large corporations from various industry sectors like commercial banking, telecommunications, Internet service providers, and other service providers over the Internet and securities firms. A majority of the contracts include the purchase of Internet gateway, client PC, and server products as described above.

Latin America

Overview. Our Latin America Region (LAR) includes the countries located in South America, Central America, the Caribbean, as well as Mexico. Trend Micro has established offices in Mexico and Brazil. Products are sold through a network of distributors and resellers.

Our Latin America net sales accounted for approximately 3% of our net sales or (Yen)1.9 billion in 2005, approximately 3% of our net sales or (Yen)2.0 billion in 2004 and approximately 3% or (Yen)1.5 billion in 2003.

Distributors. The majority of Latin American revenue comes from software licenses. Principal resellers in the region are Edsi in Argentina, Antivirus expertos and Dicofra in Mexico, Ciberlynx, F9C and security web in Brazil, among others.

Latin America s region revenue comes mainly from midsize and large enterprise markets, our customers in the Latin includes several midsize commerce enterprises, government agencies, and large corporations from commercial banking, energy, securities and telecommunication sectors.

OPERATIONS

In Japan, we outsource assembly, packaging and shipping of all of our anti-virus software products to value-added resellers. Our Taiwanese subsidiary and, in some cases, third-party service providers assemble, package, and ship products to be sold in the United States, Europe, and Asia other than Japan. Software products are generally shipped within seven days of receipt of an order and hardware products are generally shipped within ten days. Accordingly, there is some minimal order backlog at all times.

LEGAL PROCEEDINGS

On March 3, 2006, a complaint entitled *Deutsche Telecom AG versus Trend Micro Incorporated and Trend Micro Deutschland GmbH* was filed in the Regional Court of Hamburg, Germany. The lawsuit alleges trademark violations in connection with Trend Micro s use of a t-ball device in the European Union (EU). The complaint seeks to enjoin Trend Micro s standalone use of the t-ball device in the EM and an unspecified amount of damages.

We are involved in normal claims and other legal proceedings in the ordinary course of business, and are not involved in any litigation or other legal proceedings which, if determined adversely to us, would individually or in the aggregate have a material adverse effect on us or our operations.

C. Organizational Structure.

We are not, directly or indirectly, owned or controlled by other corporations or by the Japanese government or any foreign government. The following table lists our consolidated subsidiaries as of April 30, 2006.

NAME	COUNTRY OF INCORPORATION	EQUITY HELD BY TREND MICRO DIRECTLY OR INDIRECTLY
Trend Micro Incorporated	Taiwan	100%
Trend Micro Inc.	USA	100%
Trend Micro Korea Inc.	Korea	99%
Trend Micro Italy S.r.l.	Italy	100%
Trend Micro Deutschland GmbH	Germany	100%
Trend Micro Australia Pty. Ltd.	Australia	100%
Trend Micro do Brasil Ltda.	Brazil	99%
Trend Micro France SA	France	99%

Trend Micro Hong Kong Limited	China	100%
Trend Micro Latinoamerica S.A. de C.V.	Mexico	100%
Trend Micro (UK) Limited	UK	100%
Trend Micro (China) Incorporated	China	100%
Servicentro TMLA, S.A. de C.V.	Mexico	100%
Trend Micro (EMEA) Limited	Ireland	100%
Trend Micro (Singapore) Private Limited	Singapore	100%
Trend Micro (NZ) Limited	NZ	100%
Trend Micro Malaysia Sdn. Bhd.	Malaysia	99%
Trend Micro (Thailand) Limited	Thailand	91%
Trend Micro India Private Limited	India	100%

D. Property, Plants and Equipment.

Our headquarters is located in Tokyo, Japan, where we lease an aggregate of 3,897 square meters of office space under a lease contract which expires in April 2007. We also lease an aggregate of approximately 581 square meters of office space in Osaka, Fukuoka, and Nagoya.

We lease an aggregate of approximately 104,195 square feet of office space in Taipei, Taiwan, under a lease which expires in November 2006 for our regional sales, research and development and sales office. We also lease an aggregate of approximately 63,881 square feet of office space in Manila, Philippines, under a lease which expires in January 2006 and May 2006 for our customer service center. We also lease approximately 37,492 square feet of office space in Cupertino, California, U.S.A., under a lease which expires in January 2009 for research and development and sales office. We also lease small sales offices in Argentina, Australia, Benelux, Brazil, China, France, Germany, Hong Kong, India, Italy, Malaysia, Thailand, Mexico, Middle East-Africa, Norway, Singapore, South Korea, Spain and Sweden.

Item 4A. Unresolved Staff Comments

We are a large accelerated filer as defined in Rule 12b-2 under the Securities Exchange Act of 1934. There are no written comments which have been provided by the staff of the Securities and Exchange Commission regarding our periodic reports under that Act not less than 180 days before the end of the fiscal year ended December 31, 2005 and which remain unresolved as of the date of the filing of this Form 20-F with the Commission.

Item 5. Operating and Financial Review and Prospects.

A. Operating Results.

You should read the following discussion together with the financial statements and notes included in this annual report. Additionally, the following discussion includes forward-looking statements about our business and future performance. These forward-looking statements are based on our current assumptions and beliefs in light of the information currently available to us, and involve known and unknown risks and uncertainties. You should read these forward-looking statements together with the description of the risks and uncertainties associated with these statements contained under the headings Cautionary Statement Regarding Forward-Looking Statements immediately following the cover page and under Item 4.D. of this annual report.

RESTATEMENTS

In response to a comment from the staff of the Securities and Exchange Commission, as disclosed in Note 2 to our consolidated financial statements, we have restated the statements of income for the fiscal year ended December 31, 2003 and 2004 in order to reclassify maintenance costs previously reported as part of the research and development and maintenance costs within operating expenses and customer support expenses also previously included in operating expenses, into cost of sales. Furthermore, we have restated the pro forma stock compensation disclosures required by FAS 123 as amended by FAS 148 for the fiscal year ended December 31, 2003 and 2004 in order to reflect the corrections in the amortization period, expected life assumptions and volatilities used to determine pro forma stock-based compensation expense.

OVERVIEW

Strategy

We develop, market and support anti-virus software and management solutions for corporate computer systems and desktop personal computers. In the anti-virus industry there are two U.S. competitors having a higher global market share than we. These companies have strong brand-name recognition and sales forces especially outside Japan because they have longer histories in the industry. They are also developing businesses supported by management resources larger than ours, including work forces and financial strength. Under such circumstances, we aim for further growth by developing original solutions which respond to the evolution of computer viruses faster than our competitors by concentrating our management resources, by improving our superiority in products and services with additional improvements in the specifications and performance of our products from the view point of customers, and by strengthening customers loyalty with our marketing development which is conscious of customer attributes characterized by the differences in purchasing behavior.

To enhance our competency, we acquired Intermute Inc. which provides anti-spyware technologies and Kelkea Inc. which provides IP filtering and reputation services in 2005.

While we specialize in the antivirus area, we have formed several alliances with dominant vendors in areas other than antivirus solutions. In 2004, we announced affiliation with Cisco Systems, the world s largest network equipment vendor. As a result of the strategic alliance, we have put our antivirus solutions on the market as internal functions of Cisco s routers, switches and security appliance products from 2005. We believe that this sort of strategic alliance plays an important role in our sales strategy since we expect combined products to be more competitive and our and our partners sales channels to complement each other.

Critical Accounting Estimates

The methods, estimates and judgments we use in applying our accounting policies have a significant impact on the results we report in our financial statements, which we discuss under Results of Operations below. Some of our accounting policies require us to make difficult and subjective judgments, often as a result of the need to make estimates of matters that are inherently uncertain. Our most critical accounting estimates include: judgment for revenue recognition which impacts our net sales; estimate of allowance for sales returns and allowance for doubtful accounts, which impacts our sales return provision and doubtful accounts provision; recognition and measurement of income tax, current and deferred income tax assets and liabilities, which impacts our tax provision; valuation of goodwill and other intangible assets which impacts our goodwill and impairment loss. We discuss these policies further, as well as the estimates and judgments involved, below.

Revenue Recognition

We account for the licensing of software in accordance with Statement Of Position (SOP) 97-2, *Software Revenue Recognition* , released by the American Institute of Certified Public Accountants. The application of SOP 97-2 requires judgment, including whether a software arrangement includes multiple elements, and if so, whether vendor-specific objective evidence (VSOE) of fair value exists for those elements. End users receive certain elements of our products over a period of time. These elements include post-contract customer support services which includes virus pattern updates, unspecified product version updates, and telephone and online technical support, the fair value of which is recognized ratably over the service period. We allocate revenue to post-contract customer support services based on the fair value of the post-contract customer support services, which is determined based on separate renewal sales to customers. Changes to the elements in a software arrangement, the ability to identify VSOE for those elements and the fair value of the respective elements could materially impact the amount of earned and unearned revenue.

Allowance for Sales Returns and Allowance for Doubtful Accounts

We primarily sell retail packages through intermediaries. After sale of a retail package, we may approve certain returns from intermediaries or end-users. Therefore, we must make estimates of potential future product returns related to current period product revenue. We analyze historical returns, current economic trends, and changes in customer demand and acceptance of our products when evaluating the adequacy of the sales returns. Significant management judgments and estimates must be made and used in connection with establishing the sales returns in any accounting period. Material differences may result in the amount and timing of our revenue for any period if management made different judgments or utilized different estimates. Similarly, we must make estimates of the uncollectability of our accounts receivables. We specifically analyze accounts receivable and analyzes historical bad debts, customer concentrations, customer credit-worthiness, current economic trends and changes in our customer payment terms when evaluating the adequacy of the allowance for doubtful accounts. The balance of allowance for doubtful accounts and sales returns were (Yen)282 million ($2,392 thousand) and (Yen)422 million ($3,580 thousand) as of December 31, 2005, respectively. Our accounts receivable balance was (Yen)19,199 million ($162,702 thousand), net of allowance for doubtful accounts and sales returns of (Yen)704 million ($5,972 thousand), as of December 31, 2005.

Income Taxes

As part of the process of preparing our consolidated financial statements, we are required to estimate our income taxes in each of the jurisdictions in which we operate. This process involves our estimating our actual current tax exposure together with assessing temporary differences resulting from differing treatment of items, such as deferred revenue, for tax and accounting purposes. These differences result in deferred tax assets and liabilities, which are included within our consolidated balance sheet. We must then assess the likelihood that our deferred tax assets will be recovered from future taxable income. To the extent we believe that recovery is not likely, we must establish a valuation allowance. To the extent we establish a valuation allowance or increase this allowance in a period, we must include an expense within the tax provision in the statement of operations.

Significant management judgment is required in determining our provision for income taxes, our deferred tax assets and liabilities and any valuation allowance recorded against our net deferred tax assets. We have recorded this valuation allowance of (Yen)21 million ($177 thousand) as of December 31, 2005, due to uncertainties related to our ability to utilize some of our deferred tax assets, primarily consisting of certain net operating losses carried forward. The valuation allowance is based on our estimates of taxable income by jurisdiction in which we operate and the period over which our deferred tax assets will be recoverable. In the event that actual results differ from these estimates or we adjust these estimates in future periods we may need to establish an additional valuation allowance which could materially impact our financial position and results of operations.

The net deferred tax asset as of December 31, 2005 was (Yen)8,761 million ($74,243 thousand), net of a valuation allowance of (Yen)21 million ($177 thousand).

Valuation of Goodwill and other intangible assets

Goodwill is the excess of the purchase price of the acquired business over the fair value of its net tangible and identifiable intangible assets. Other intangible assets consist primarily of existing technology purchased by business acquisition. In determining the purchase price of acquired business and existing technology, management is required to make significant estimates of the fair values of assets acquired and liabilities assumed, especially with respect intangible assets. These estimates are based on the information obtained from the management of the acquired companies to and include the cash flows that an asset is expected to generate in the future, the weighted average cost of capital, and cost savings expected to be derived from acquiring asset. These estimates are inherently uncertain and unpredictable.

The balance of goodwill and existing technology were (Yen)2,130 million ($18,053 thousand) and (Yen)615 million ($5,212 thousand) as of December 31, 2005, respectively. We assess the impairment of goodwill annually, or more often if events or changes in circumstances indicate that the carrying value may not be recoverable. We assess the impairment of other intangible assets whenever events or changes in circumstances indicate that its carrying amount may not be recoverable. An impairment loss would be recognized when the sum of the future net cash flows expected to result from the use of the asset and its eventual disposition is less than its carrying amount. Such impairment loss would be measured as the difference between the carrying amount of the assets and its fair value. The estimate of cash flow is based on, among other things, certain assumptions about expected future operating performance and an appropriate discount rate determined by our management. Our estimates of discounted cash flows may differ from actual cash flows due to economic conditions, changes to the business model, or changes in operating performance. If management made different estimates, material differences may result in write-downs of goodwill and intangible assets, which would be reflected by charges to our operating results for any period presented.

EFFECT ON OUR RESULTS OF OPERATIONS FROM DISTRIBUTION OF A DEFECTIVE VIRUS PATTERN FILE IN APRIL 2005

As described under in Item 4.B. - *Distribution of a Defective Virus Pattern File in April 2005*, we distributed a defective virus file pattern that resulted in damage to the computers of our customers who downloaded the file. As described in Item 4.B., we took steps to resolve our customers problems and ensure that a similar problem would not recur. We have incurred (Yen) 991 million ($8,398 thousand) related to this issue for the year ended December 31, 2005 as cost of sales and operating expenses. There is some possibility of incurring further cost, however Management expects additional cost will be insignificant.

RESULTS OF OPERATIONS

Our consolidated financial statements are denominated in Japanese yen. All asset and liability accounts of our foreign subsidiaries are translated into Japanese yen at the year-end rates of exchange. We translate all income and expense accounts at rates of exchange that approximate those prevailing at the time of the transactions and accumulate the resulting adjustments as a separate component of shareholders equity. We translate foreign currency-denominated receivables and payables into Japanese yen at year-end rates of exchange and recognize or expense the resulting translation gains or losses on a current basis. Fluctuations in the exchange rate between the Japanese yen and other currencies, principally the U.S. dollar, Euro and the New Taiwan dollar, will affect the translation of the financial results of our foreign subsidiaries into Japanese yen for purposes of our consolidated financial results, and will also affect the Japanese yen value of any amounts we receive from our subsidiaries.

The following table sets forth certain consolidated statements of income data as a percentage of net sales for the periods indicated:

	Years ended December 31,		
	2003	2004	2005
	(Restated)(1)	(Restated)(1)	
Net sales	100.0%	100.0%	100.0%
Cost of sales			
Amortization of capitalized software, and Materials	6.6%	5.2%	3.5%
Maintenance	4.6%	3.7%	2.3%
Customer support	10.0%	9.2%	9.4%
Total Cost of sales	21.2%	18.1%	15.2%
Operating expenses:			
Selling	31.9%	25.8%	28.7%
Research and development	3.6%	4.2%	6.0%
General and administrative	11.8%	9.9%	12.3%
Total operating expenses	47.3%	39.9%	47.0%
Operating income	31.5%	42.0%	37.8%

(1) See Note 2 (1) to the consolidated financial statements.

Our Revenue Structure

Our revenue is derived primarily from product revenue, which includes software product license and post-contract customer support (PCS) services. Product revenue includes limited sales of our products to other companies for inclusion in their products. Revenue from our post-contract customer support services, which includes virus pattern updates, product version updates, telephone and online technical support, is deferred and recognized ratably over the service period. We allocate revenue to post-contract customer support services based on the fair value of the post-contract customer support services, which are determined based on separate sales of renewals to customers. Upon expiration of the initial term, corporate end users can renew the post-contract customer support services annually by paying a fee generally equal to one-half of the initial license fee in Japan and between 20% and 50% of the initial license fee in the United States and elsewhere, depending on the country. For retail purchasers of PC-cillin/Virus Buster, the license fee includes post-contract customer support services for the initial one-year term only. In order to receive post-contract customer support services after the initial term, these retail purchasers must pay a percentage, generally less than one-half, of the original license fee.

We generally recognize revenues from software product licenses when:

persuasive evidence of an arrangement exists;

the product has been delivered;

the fee is fixed and determinable; and

collection of the resulting receivable is reasonably assured.

In general, we record sales revenues attributable to post-contract customer support services as deferred revenue and recognize such revenues ratably over the license term. The percentage of the license fee which is deferred varies depending on the location of the Trend Micro entity making the sale, as well as the product sold.

In our operations, maintenance costs and customer support expenses, which were previously included in operating expenses, are disclosed as cost of sales from the year ended December 31, 2005 and prior year figures have been reclassified. Thus, there are three lines under cost of sales; Amortization of capitalized software and Materials, Maintenance and Customer support. Amortization of capitalized software and Materials consists of outbound shipping and handling costs, costs of producing manuals and packaging, and amortization of software development costs. Maintenance costs represent the costs incurred for not only simple program-bug-fixing but also minor version-ups in the product sustain stage of out anti-virus software product development cycle. Customer support costs represent the costs incurred in connection with Virus Pattern File development and update activities as along with other customer support activities such as trouble shooting, emerging virus information gathering and product defect information gathering.

We operate our business in five geographic regions: Japan, Europe, North America, Asia Pacific and Latin America. Japan accounted for around 40% and, together with Europe and North America, over 80% of our net sales for each of our last three fiscal years.

Sales by Product and Service

The following table sets forth net sales by products and services for the periods indicated:

	2003		2004		2005			Year over Year Growth	
	(in millions of yen and thousands of U.S. dollars, except percentages)							2004	2005
Server based	(Yen) 3,633	8%	(Yen) 3,310	5%	(Yen) 3,279	$ 27,784	4%	-9%	-1%
Personal Computer	13,507	28%	16,890	27%	19,714	167,072	27%	25%	17%
Retail sales	8,141	17%	12,384	20%	15,346	130,053	21%	52%	24%
Site license sales	5,366	11%	4,506	7%	4,368	37,019	6%	-16%	-3%
Internet based	10,752	22%	16,647	27%	18,374	155,710	25%	55%	10%
All Suite products	9,914	21%	18,597	30%	24,485	207,500	34%	88%	32%
PCS*1 and Royalties	9,215	19%	4,714	8%	3,683	31,214	5%	-49%	-22%
Other	1,067	2%	1,891	3%	3,495	29,617	5%	77%	85%
	(Yen) 48,088	100%	(Yen) 62,049	100%	(Yen) 73,030	$ 618,897	100%	29%	18%

* Post contract customer support fees

All Suite products were included in another products until 2004, however for the amounts importance, all Suite products are separately disclosed from 2005. In addition, prior figures have been reclassified.

Net sales of Server based products in 2005 decreased 1% compared with 2004 by decreased sales of Trend Micro ServerProtect. This decrease is due to the increase of the conversion to Suite products.

Within the personal computer product category, net sales of anti-virus software, including retail package sales of Trend Micro PC-cillin/Virus Buster series, increased from approximately (Yen)16,890 million in 2004 to approximately (Yen)19,714 million ($167,072 thousand) in 2005. Retail package sales of personal computer software increased due primarily to increased sales of our products, including the Virus Buster 2006 which we released in November 2005, in the Japanese market.

Net sales of internet-based products in 2005 increased 10% from 2004, reflecting mainly increased sales of InterScan Web Security Suite and InterScan Messaging Security Suite products in 2005 compared with 2004.

Net sales of All Suite products in 2005 increased 32% from 2004, reflecting mainly sales of Client/Server Suite products in 2005 compared with 2004.

Net sales of post-contract customer support fees and royalties in 2005 decreased 22% from 2004 due primarily to reclassification of the products into other revenue categories. If net sales of post-contract customer support fees and royalties in 2004 had been categorized as that in 2005 as

mentioned above, this line item would have increased 71% in 2005 compared with 2004.

Net sales of post-contract customer support fees and royalties in 2004 decreased 49% from 2003. Until 2003, the renewal sales were categorized as post-contract customer support fees and royalties in the United Sates, because their accounting system could not separate the renewal sales amount by product. Because of the improvement of the system, the renewal sales amount can now be categorized by product. For descriptive purpose to compare 2004 to 2003, if such renewal sales amount had been categorized as post-contract customer support fees and royalties in 2004 in the United States, this line item would have increased 6.2% in 2004 compared with 2003.

Net sales in 2004 increased 29% compared with 2003. The increase was due primarily to increased sales of All Suite products such as NeaTSuite or Client/Server Suite.

Net sales of internet-based products in 2004 increased 55% from 2003, reflecting mainly increased sales of InterScan products in 2004 compared with 2003. If renewal sales amount had been categorized as post-contract customer support fees and royalties in 2004 in the United States as mentioned above, this line item would have increased 38% in 2004 compared with 2003.

Net sales of Server based products in 2004 decreased 9% compared with 2003 by decreased sales of Trend Micro ServerProtect. This decrease is due to the increase of the conversion to Suite products. If renewal sales amount had been categorized as post-contract customer support fees and royalties in 2004 in the United States as mentioned above, this line item would have decreased 13% in 2004 compared with 2003.

Within the personal computer product category, net sales of anti-virus software, including retail package sales of Trend Micro PC-cillin/Virus Buster series, increased from approximately (Yen) 13,507 million in 2003 to approximately (Yen) 16,890 million in 2004. Retail package sales of personal computer software increased due primarily to increased sales of our products, including the Virus Buster 2005 which we released in October 2004, in the Japanese market. If renewal sales amount had been categorized as post-contract customer support fees and royalties in 2004 in the United States as mentioned above, this line item would have decreased 23% in 2004 compared with 2003.

Cost of sales

Cost of sales for the three years ended December 31, 2005 were as follows:

	Years ended December 31,			
	2003	2004	2005	2005
	(restated)(1)	(restated)(1)		
		Millions of yen		Thousands of U.S. dollars
Cost of sales:				
Amortization of capitalized software, and Materials	(Yen) 3,168	(Yen) 3,236	(Yen) 2,599	$ 22,022
Maintenance	2,194	2,261	1,671	14,163
Customer Support	4,831	5,724	6,858	58,118
Total Cost of sales	(Yen) 10,193	(Yen) 11,221	(Yen) 11,128	$ 94,303

(1) See Note 2 (1) to the consolidated financial statements.

Amortization of capitalized software, and Material Costs

Amortization of capitalized software and Material cost consist primarily of amortization of the capitalized software for sales and purchase of products. Amortization of capitalized software, and Material costs decreased (Yen)637 million, or -20%, in 2005 compared with 2004, and increased (Yen) 68 million, or 2%, in 2004 compared with 2003.

Maintenance Expenses

Maintenance expenses consist primarily of payroll and related expenses for software engineers who update our anti-virus software products. Maintenance expenses decreased (Yen) 590 million, or -26%, in 2005 compared with 2004, and increased (Yen) 67 million, or 3%, in 2004 compared with 2003. Maintenance costs are the costs related to product version updates to enable our customers to cope with newly prevailing computer viruses and bug fixing and are expensed as incurred.

The number of employees at our maintenance department was 108 as of December 31, 2003, 114 as of December 31, 2004, and 130 as of December 31, 2005.

Customer Support Expenses

Customer support expenses consist primarily of payroll, related expenses and outsourced customer service fees. Customer support expenses increased (Yen) 1,134 million, or 20%, in 2005 compared with 2004, and increased (Yen) 893 million, or 18%, in 2004 compared with 2003.

Compared to 2004, the number of employees in our customer support department increased by 98 in Asia Pacific. It is due to an expansion of the customer support centers in the Philippines to meet the satisfaction of our global customers. The expansion was for enterprise products such as outbreak prevention services and damage cleanup services based on the Trend Micro Enterprise Strategy described Item 4.B of this annual report, and the recent expansion of the services provided to customers by our customer support department. Additionally, due to the trouble caused by the virus pattern file we distributed on April 23, 2005, it also includes costs to assist for reconstruction and to settle the problem for our customers.

Operating Expenses

Operating expenses for the three years ended December 31, 2005 were as follows:

	Years ended December 31,			
	2003	2004	2005	2005
	(restated)(1)	(restated)(1)		
		Millions of yen		Thousands of U.S. dollars
Operating expenses:				
Selling	(Yen) 15,360	(Yen) 16,009	(Yen) 20,944	$ 177,496
Research and development	1,725	2,597	4,395	37,247
General and administrative	5,656	6,144	8,991	76,192
Total operating expenses	(Yen) 22,741	(Yen) 24,750	(Yen) 34,330	$ 290,935

(1) See Note 2 (1) to the consolidated financial statements.

Selling Expenses

Selling expenses consist primarily of advertising, selling commissions, payroll and related expenses of sales and marketing department. Selling expenses increased (Yen)4,935 million, or