CHECK POINT SOFTWARE TECHNOLOGIES LTD
Form 20-F
March 05, 2009

SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 20-F

o REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR (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, 2008

OR

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

For the transition period from _____ to _____

OR

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

Date of event requiring this shell company report.....

Commission file number 000-28584

CHECK POINT SOFTWARE TECHNOLOGIES LTD.

(Exact name of Registrant as specified in its charter)

ISRAEL

(Jurisdiction of incorporation or organization)

5 Ha'Solelim Street, Tel Aviv 67897, Israel

(Address of principal executive offices)

John Slavitt, Esq.
General Counsel
Check Point Software Technologies, Inc.
800 Bridge Parkway
Redwood City, CA 94065 U.S.A.
Tel: (650) 628-2110
Fax: (650) 649-1975

(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

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

Title of each class	Name of exchange on which registered
Ordinary shares, NIS 0.01 nominal value	NASDAQ Global Select Market

Securities registered or to be registered pursuant to Section 12(g) of the Act. None

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act. None

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. 210,042,282 ordinary shares, NIS 0.01 nominal value

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 o

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 o No x

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 o

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

Large Accelerated filer x Accelerated filer o Non-accelerated filer o

Indicate by check mark the basis of accounting the registrant has used to prepare the financial statements included in this filing:

x U.S. GAAP

o International Financial Reporting Standards as issued by the International Accounting Standards Board

o Other

If Other has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow.

Item 17 o Item 18 o

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act):

Yes o No x

TABLE OF CONTENTS

PART I

Currency of Presentation and Certain Defined Terms

In this Annual Report on Form 20-F, references to U.S. or United States are to the United States of America, its territories and possessions. References to $", dollar or U.S. dollar are to the legal currency of the United States of America; references to NIS or Israeli Shekel are to the legal currency of Israel; references to Euro are to the legal currency of the European Union; and references to SEK or Swedish Krona are to the legal currency of Sweden.

All references to we, us, our or Check Point shall mean Check Point Software Technologies Ltd., and, unless specifically indicated otherwise or the context indicates otherwise, our consolidated subsidiaries.

Forward-Looking Statements

Some of the statements contained in this Annual Report on Form 20-F are forward-looking statements that involve risks and uncertainties. The statements contained in this Annual Report on Form 20-F that are not purely historical are forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended, including, without limitation, statements regarding trends related to our business and our expectations, beliefs, intentions or strategies regarding the future. These statements are subject to known and unknown risks, uncertainties and other factors, which may cause our actual results to differ materially from those implied by the forward-looking statements. In some cases, you can identify forward-looking statements by terminology such as may, will, could, should, expects, plans, anticipates, believes, intends, estimates, predicts, potential, or continue or the negati comparable terminology. Forward-looking statements also include, but are not limited to, statements in (i) Item 4 Information on Check Point regarding our belief as to increased acceptance of Internet technologies, expansion of connectivity services, acceleration of the use of networks, the need and demand for network, gateway and virtual security, the need and demand for flexible and extensible security, the demand for our new blade architecture and adoption of new licensing offerings, increasing demands on enterprise security systems, the impact of our relationship with our technology partners on our sales goals, the contribution of our products to our future revenue, our development of future products, and our ability to integrate, market and sell acquired products and technologies; and (ii) Item 5 Operating and Financial Review and Prospects regarding, among other things, our expectations regarding our business and the markets in which we operate and into which we sell products, future amounts and sources of our revenue, our ongoing relationships with our current and future customers and channel partners, our future costs and expenses, the adequacy of our capital resources, and our expectations regarding the acquisition of Nokia s security appliance business.

Forward-looking statements involve risks, uncertainties and assumptions, and our actual results may differ materially from those predicted. Many of these risks, uncertainties and assumptions are described in the risk factors set forth in Item 3 Key Information Risk Factors and elsewhere in this Annual Report on Form 20-F. All forward-looking statements included in this Annual Report on Form 20-F are based on information available to us on the date of the filing and reasonable assumptions. We undertake no obligation to update any of the forward-looking statements after the date of the filing, except as required by applicable law.

PART I

ITEM 1. IDENTITY OF DIRECTORS, SENIOR MANAGEMENT AND ADVISERS

Not applicable.

ITEM 2. OFFER STATISTICS AND EXPECTED TIMETABLE

Not applicable.

ITEM 3. KEY INFORMATION

Selected Financial Data

We prepare our historical consolidated financial statements in accordance with accounting principles generally accepted in the United States (U.S. GAAP). The selected financial data, set forth in the table below, have been derived from our audited historical financial statements for each of the years from 2004 to 2008. The selected consolidated statement of income data for the years 2006, 2007, and 2008, and the selected consolidated balance sheet data at December 31, 2007 and 2008, have been derived from our audited consolidated financial statements set forth in Item 18 Financial Statements. The selected consolidated statement of income data for the years 2004 and 2005, and the selected consolidated balance sheet data at December 31, 2004, 2005 and 2006, has been derived from our previously published audited consolidated financial statements, which are not included in this Annual Report on Form 20-F. This selected financial data should be read in conjunction with our consolidated financial statements, and are qualified entirely by reference to such consolidated financial statements.

	Year Ended December 31,				
	2004	2005	2006	2007	2008
	(in thousands, except per share data)				
Consolidated Statement of Income Data:					
Revenues	$ 515,360	$ 579,350	$ 575,141	$ 730,877	$ 808,490
Operating expenses (*):					
Cost of revenues	27,750	30,540	36,431	82,301	92,609
Research and development	44,483	50,542	62,210	80,982	91,629
Selling and marketing	135,712	142,336	157,114	217,491	214,439
General and administrative	24,098	24,244	43,503	53,527	53,313
Acquired in-process R&D	23,098	-	1,060	17,000	-
Total operating expenses	255,141	247,662	300,318	451,301	451,990
Operating income	260,219	331,688	274,823	279,576	356,500
Financial income, net	44,777	54,177	63,647	49,725	40,876
Other-than-temporary impairment of marketable securities (**)	-	-	-	-	(11,221)
Income before taxes on income	304,996	385,865	338,470	329,301	386,155
Taxes on income	56,603	66,181	60,443	48,237	62,189
Net income	$ 248,393	$ 319,684	$ 278,027	$ 281,064	$ 323,966
Basic earnings per share	$ 0.99	$ 1.30	$ 1.18	$ 1.26	$ 1.51
Shares used in computing basic earnings per share	251,244	245,520	235,519	222,548	214,361
Diluted earnings per share	$ 0.95	$ 1.27	$ 1.17	$ 1.25	$ 1.50
Shares used in computing diluted earnings per share	260,608	251,747	236,769	225,442	216,668

* Including pre-tax charges for amortization of intangible assets, acquisition related expenses and stock-based compensation in the following items:

Amortization of intangible assets and acquisition related expenses					
Cost of revenues	$ 4,061	$ 5,414	$ 5,414	$ 27,724	$ 24,554
Selling and marketing	171	228	604	12,260	12,428
General and administrative	-	-	927	-	
Total	$ 4,232	$ 5,642	$ 6,945	$ 39,984	$ 36,982
Stock-based compensation					
Cost of products and licenses	$ -	$ -	$ 39	$ 65	$ 48
Cost of software updates, maintenance and services	137	408	470	668	684
Research and development	1,297	1,252	9,371	4,309	5,037
Selling and marketing	2,745	1,825	7,997	8,780	6,855
General and administrative	441	260	18,515	20,230	19,703
Total	$ 4,620	$ 3,745	$ 36,392	$ 34,052	$ 32,327

** Year ended December 31, 2008, includes non-cash write down of $11.2 million (pre-tax) of marketable securities in accordance with SFAS 115.

	December 31,				
	2004	2005	2006	2007	2008
	(in thousands)				
Consolidated Balance Sheet Data:					
Working capital	$ 791,455	$ 1,186,119	$ 967,805	$ 692,316	$ 791,976
Total assets	1,919,819	2,092,495	2,080,793	2,368,575	2,593,616
Shareholders' equity	1,630,824	1,775,721	1,711,533	1,856,955	2,015,865
Capital stock	370,017	387,303	423,155	465,104	504,182

Risk Factors

If any of the following risks actually occurs, our business, financial condition, results of operations, and future prospects could be materially and adversely affected. In that event, the market price of our ordinary shares could decline and you could lose part or all of your investment.

Risks Related to Our Business and Our Market

If the market for information and network security solutions does not continue to grow, our business will be adversely affected

The market for our products has continued to expand but the market for information and network security solutions may not continue to grow. Continued growth of this market will depend, in large part, upon:

- The continued expansion of Internet usage and the number of organizations adopting or expanding intranets.
- The ability of their respective infrastructures to support an increasing number of users and services.

- The continued development of new and improved services for implementation across the Internet and between the Internet and intranets.
- The adoption of data security measures as it pertains to data encryption technologies.
- Government regulation of the Internet and governmental and non-governmental requirements and standards with respect to data security and privacy.
- General economic conditions in the markets in which we, our customers and our suppliers operate.

During the current global economic slowdown, many companies have reduced expenditures, and adverse economic conditions may cause our customers to reduce or postpone their technology spending significantly, which could result in reductions in sales of our products, longer sales cycles, slower adoption of new technologies and increased price competition.

If the necessary infrastructure or complementary products and services are not developed in a timely manner and, consequently, the enterprise security, data security, Internet, or intranet markets fail to grow or grow more slowly than we currently anticipate, our business, operating results, and financial condition may be materially adversely affected. Additional details are provided in Item 4 Information on Check Point.

We may not be able to successfully compete

The market for information and network security solutions is intensely competitive and we expect that competition will continue to increase in the future. Our principal competitors include Cisco Systems, Inc., Fortinet Inc. and Juniper Networks, Inc. We also compete with several other companies, including McAfee, Inc., Microsoft Corporation, SonicWall Inc. and Symantec Corporation with respect to specific products that we offer, including data security products.

Some of our current and potential competitors have various advantages over us, including longer operating histories; access to larger customer bases; significantly greater financial, technical and marketing resources; a broader portfolio of products, applications and services; and larger patent and intellectual property portfolios. As a result, they may be able to adapt better than we can to new or emerging technologies and changes in customer requirements, or to devote greater resources to the promotion and sale of their products. Furthermore, some of our competitors with more diversified product portfolios may be better able to withstand a reduction in spending on information and network security solutions. In addition, some of our competitors have greater financial resources than we do, and they have offered, and in the future may offer, their products at lower prices than we do, which may cause us to lose sales or to reduce our prices in response to competition.

In addition, consolidation in the markets in which we compete may affect our competitive position. We may not be able to continue competing successfully against our current and future competitors. Increased competition may result in price reductions, reduced gross margins, and loss of market share, any of which will materially adversely affect our business, operating results, and financial condition.

The markets in which we compete also include many niche competitors, generally smaller companies at a relatively early stage of operations, which are focused on specific Internet and data security needs. These companies specialized focus may enable them to adapt better than we can to new or emerging technologies and changes in customer requirements in their specific areas of focus. In addition, some of these companies can invest relatively large resources on very specific technologies or customer segments. The effect of these companies activities in the market may result in price reductions, reduced gross margins and loss of market share, any of which will materially adversely affect our business, operating results, and financial condition.

Further, vendors of operating system software or networking hardware may enhance their products to include functionality that is currently provided by our products. The widespread inclusion of similar functionality to that which is offered by our solutions, as standard features of operating system software or networking hardware, could significantly reduce the marketability of our products, particularly if the quality of such functionality were comparable to that of our products. Furthermore, even if the network or application security functionality, provided as standard features by operating systems software or networking hardware, is more limited than that of our solutions, a significant number of customers may elect to accept more limited functionality in lieu of purchasing additional products.

If any of the events described above occur, our business, operating results and financial condition could be materially adversely affected. Additional details are provided in Item 4 Information on Check Point.

If we fail to enhance our existing products, develop or acquire new and more technologically advanced products, or fail to successfully commercialize these products, our business and results of operations will suffer

The information and network security industry is characterized by rapid technological advances, changes in customer requirements, frequent new product introductions and enhancements, and evolving industry standards in computer hardware and software technology. In particular, the markets for data security, Internet, and intranet applications are rapidly evolving. As a result, we must continually change and improve our products in response to changes in operating systems, application software, computer and communications hardware, networking software, programming tools, and computer language technology. Further, we must continuously improve our products to protect our customers data and networks from evolving security threats.

Our future operating results will depend upon our ability to enhance our current products and to develop and introduce new products on a timely basis; to address the increasingly sophisticated needs of our customers; and to keep pace with technological developments, new competitive product offerings, and emerging industry standards. Our competitors introduction of products embodying new technologies and the emergence of new industry standards may render our existing products obsolete or unmarketable. While we have been successful in developing, acquiring, and marketing new products and product enhancements that respond to technological change and evolving industry standards, we may not be able to continue to do so. In addition, we may experience difficulties that could delay or prevent the successful development, introduction, and marketing of these products, as well as the integration of acquired products. Furthermore, our new products or product enhancements may not adequately meet the requirements of the marketplace or achieve market acceptance. In some cases, a new product or product enhancements may negatively affect sales of our existing products. If we do not respond adequately to the need to develop and introduce new products or enhancements of existing products in a timely manner in response to changing market conditions or customer requirements, our business, operating results and financial condition may be materially adversely affected. Additional details are provided in Item 4 Information on Check Point and under the caption We may not be able to successfully compete in this Item 3 Key Information Risk Factors.

Product defects may increase our costs and impair the market acceptance of our products and technology

Our products are complex and must meet stringent quality requirements. They may contain undetected hardware or software errors or defects, especially when new or acquired products are introduced or when new versions are released. In particular, the personal computer hardware environment is characterized by a wide variety of non-standard configurations that make pre-release testing for programming or compatibility errors very difficult and time-consuming. We may need to divert the attention of our engineering personnel from our research and development efforts to address instances of errors or defects. In addition, we may in the future incur costs associated with warranty claims.

Our products are used to deploy and manage Internet security and protect information, which may be critical to organizations. As a result, the sale and support of our products entails the risk of product liability and related claims. We do not know whether, in the future, we will be subject to liability claims or litigation for damages related to product errors, or will experience delays as a result of these errors. Our sales agreements and product licenses typically contain provisions designed to limit our exposure to potential product liability or related claims. In selling our products, we rely primarily on shrink wrap licenses that are not signed by the end user, and for this and other reasons, these licenses may be unenforceable under the laws of some jurisdictions. As a result, the limitation of liability provisions contained in these licenses may not be effective. Although we maintain product liability insurance for most of our products, the coverage limits of these policies may not provide sufficient protection against an asserted claim. If litigation were to arise, it could, regardless of its outcome, result in substantial expense to us, significantly divert the efforts of our technical and management personnel, and disrupt or otherwise severely impact our relationships with current and potential customers. In addition, if any of our products fail to meet specifications or have reliability, quality or compatibility problems, our reputation could be damaged significantly and customers might be reluctant to buy our products, which could result in a decline in revenues, a loss of existing customers, and difficulty attracting new customers.

We are subject to risks relating to acquisitions

We have made acquisitions in the past and we may make additional acquisitions in the future. The pursuit of acquisitions may divert the attention of management and cause us to incur various expenses in identifying, investigating, and pursuing suitable acquisitions, whether or not they are consummated.

Competition within our industry for acquisitions of businesses, technologies, assets and product lines has been, and may in the future continue to be, intense. As such, even if we are able to identify an acquisition that we would like to consummate, we may not be able to complete the acquisition on commercially reasonable terms or because the target is acquired by another company. Furthermore, in the event that

we are able to identify and consummate any future acquisitions, we could:

- Issue equity securities which would dilute current shareholders' percentage ownership;
- Incur substantial debt;
- Assume contingent liabilities; or
- Expend significant cash.

These financing activities or expenditures could harm our business, operating results and financial condition or the price of our ordinary shares. Alternatively, due to difficulties in the capital and credit markets, we may be unable to secure capital on acceptable terms, or at all, to complete acquisitions.

In addition, if we acquire additional businesses, we may not be able to integrate the acquired personnel, operations, and technologies successfully or effectively manage the combined business following the completion of the acquisition. We may also not achieve the anticipated benefits from the acquired business due to a number of factors, including:

- Unanticipated costs or liabilities associated with the acquisition.
- Incurrence of acquisition-related costs.
- Diversion of management s attention from other business concerns.
- Harm to our existing business relationships with manufacturers, distributors and customers as a result of the acquisition.
- The potential loss of key employees.
- Use of resources that are needed in other parts of our business.
- Use of substantial portions of our available cash to consummate the acquisition.
- Unrealistic goals or projections for the acquisition.

Moreover, even if we do obtain benefits from acquisitions in the form of increased sales and earnings, there may be a delay between the time when the expenses associated with an acquisition are incurred and the time when we recognize such benefits.

In December 2006, we completed the acquisition of NFR Security, Inc., a U.S. privately held company. In January 2007, we completed the acquisition of Protect Data AB (Protect Data), which was a public company listed on the Stockholm Stock Exchange, and completed the integration of Protect Data into Check Point s business. Protect Data is the owner of 100% of Pointsec Mobile Technologies AB (Pointsec), a leading provider of data security products, and other subsidiaries, as listed below in Item 4 Information on Check Point under the caption Organizational structure. Pointsec provides products that are different in nature than our core technologies, including encryption software that helps companies secure data that may be stored on employee laptops, personal computers, smartphones, and personal digital assistants (PDAs).

On December 22, 2008, we entered into an Asset Purchase Agreement with Nokia, Inc. (Nokia) to acquire Nokia s security appliance business. The pending acquisition is expected to close in the first or second quarter of 2009 and is subject to regulatory approvals and customary closing conditions. If and when we close this pending acquisition, we expect to expand our security appliance line of business. However, we cannot assure you that we will complete the acquisition or successfully integrate the acquired personnel, operations and technologies or that we will be able to effectively manage the combined business following the completion of the acquisition.

If we are unable to successfully address any of the risks related to acquisitions, our business, financial condition or operating results could be harmed.

Our operating margins may decline

We may experience future fluctuations or declines in operating margins from historical levels due to many factors, including:

- Increased competition that results in pressure on us to reduce prices.
- Additional investments in the continuing development and expansion of our sales and marketing organization, including the expansion and further reinforcement of our worldwide field organization.
- Integration of an acquired business that at the time of acquisition has operating margins lower than ours.
- Additional expansion of our research and development organization.
- Expected growth in the percentage of revenues that we derive from products incorporating hardware, which have lower operating margins than software products.
- Global economic conditions that results in changes in customer capital spending budget.

Our operating margins are likely to fluctuate based on the amount and timing of these and other developments. In addition, if our revenue levels are below expectations, this will likely have an adverse effect on our operating margins, since most of our expenses are not variable in the short term.

Our quarterly operating results are likely to fluctuate which could cause us to miss expectations about these results and cause the trading price of our ordinary shares to decline

Our revenues from our sales are not consistent from quarter to quarter and we experience some degree of seasonality in our sales. In addition, a majority of our sales typically occur in the last month of each quarter. Factors that could cause our revenues and operating results to fluctuate from period to period include:

- Changes in customer capital spending budgets and allocations throughout the year.
- General economic conditions in the markets in which our customers operate.
- Seasonal trends in customer purchasing.
- Competitive market conditions, including the pricing actions of our competitors.
- The occurrence of an infrastructure failure resulting in delay of quarter-end purchases of products.

- The occurrence of Internet security breaches or threats.
- The timing and success of new products and new technologies introduced by us or our competitors.
- Regional or global economic and political conditions.
- Changes in our operating expenses and extraordinary expenses.
- Impairment of goodwill and intangibles.
- Our relationships with, and sales through, our channel partners.

- Our ability to integrate the technology and operations of acquired businesses with our own business.

- Fluctuations in foreign currency exchange rates.

Unfavorable changes in the factors listed above, many of which are outside of our control, could materially adversely affect our business, operating results, and financial condition.

Historically, our revenues have reflected seasonal fluctuations. Typically, we experience a slowdown in sales of our products in the third quarter and an increase in sales in the fourth quarter. We believe that we will continue to encounter quarter-to-quarter fluctuations.

We operate with minimal backlog of products. Therefore, the timing and volume of orders within a given period and our ability to fulfill these orders, determine the amount of our product revenues within the period.

We derive our sales primarily through indirect channels, making it difficult for us to predict revenues because we depend partially on estimates of future sales provided by third parties. In addition, changes in our arrangements with our network of channel partners or in the products they offer, such as our recent introduction of new support programs and products for our customers, which combine support from our channel partners with back-end support from us, could affect the timing and volume of orders. Furthermore, our expense levels are based, in part, on our expectations as to future revenues. If our revenue levels are below expectations, our operating results are likely to be adversely affected, since most of our expenses are not variable in the short term.

As a result, we believe that period-to-period comparisons of our results of operations are not necessarily meaningful and should not be relied upon as indications of future performance. Due to the factors described above, it is possible that in some future quarter, our operating results may be below the expectations of public market analysts and investors. In this event, the price of our ordinary shares would likely decline.

Continuing unfavorable national and global economic conditions could have a material adverse effect on our business, operating results and financial condition

The recent crisis in the financial and credit markets in the United States, Europe and Asia has led to a global economic slowdown, with the economies of the United States and Europe showing significant signs of weakness. If the economies in any part of the world continue to be weak or weaken further, our customers may reduce or postpone their spending significantly. This could result in reductions in sales of our products or services and longer sales cycles, slower adoption of new technologies and increased price competition. In addition, weakness in the end-user market could negatively affect the cash flow of our distributors and resellers who could, in turn, delay paying their obligations to us. This would increase our credit risk exposure and cause delays in our recognition of revenues on future sales to these customers. Specific economic trends, such as declines in the demand for PCs, servers, and other computing devices, or weakness in corporate information technology spending, could have a more direct impact on our business. Any of these events would likely harm our business, operating results and financial condition. If global economic and market conditions, or economic conditions in the United States or other key markets do not improve, or continue to deteriorate, it may have a material adverse effect on our business, operating results and financial condition.

We may fail to maintain effective internal controls in accordance with Section 404 of the Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 imposes certain duties on us and our executives and directors. Our efforts to comply with the requirements of Section 404, which started in connection with our 2006 Annual Report on Form 20-F, have resulted in increased general and administrative expense and a diversion of management time and attention, and we expect these efforts to require the continued commitment of resources. Section 404 of the Sarbanes-Oxley Act requires (i) management s annual review and evaluation of our internal control over financial reporting and (ii) an attestation report by our independent registered public accounting firm on the effectiveness of our internal control over financial reporting, in connection with the filing of the Annual Report on Form 20-F for each fiscal year. We have documented and tested our internal control systems and procedures and have made improvements in order for us to comply with the requirements of Section 404. While our assessment of our internal control over financial reporting resulted in our conclusion that as of December 31, 2008, our internal control over financial reporting was effective, and our independent registered public accounting firm has issued an unqualified attestation report on the effectiveness of our internal control over financial reporting, we cannot predict the outcome of our testing in future periods. If we fail to maintain the adequacy of our internal controls, we may not be able to ensure that we can conclude on an ongoing basis that we have effective internal control over financial reporting. Failure to maintain effective internal controls over financial reporting could result in investigation or sanctions by regulatory authorities, and could have a material adverse effect on our operating results, investor confidence in our reported financial information, and the market price of our ordinary shares.

We depend on our key personnel, including our executive officers, and the failure to attract and retain key personnel could adversely affect our business

Our future performance depends in large part on the continued service of our key technical, sales and management personnel. None of our key personnel is bound by an employment agreement requiring service for any defined period of time. If we are unable to retain members of our management and key employees, we must successfully manage transition and replacement issues that may result from such departures.

Our future performance also depends on our ability to attract skilled personnel in the future. Competition for personnel is intense. In order to retain our employees, we provide many of them with cash and stock-based awards that can be realized over time to increase longer-term commitments. However, we cannot be assured that we can retain our key personnel in the future.

The loss of services of any of our key personnel, the inability to retain and attract qualified personnel in the future, or delays in hiring required personnel, could make it difficult for us to meet key objectives, such as product deliveries, sales and customer results and meeting managerial and financial milestones, and could adversely affect our business, financial condition and results of operations.

Under current U.S., Swedish, and Israeli law, we may not be able to enforce covenants not to compete and, therefore, we may be unable to prevent our competitors from benefiting from the expertise of some of our former employees

Under current U.S., Swedish, and Israeli law, we may not be able to enforce, in whole or in part, agreements that prohibit some of our employees from competing with us or working for our competitors after they cease working for us. It may be difficult for us to restrict our competitors from gaining the expertise our former employees gained while working for us. Competitors and others have in the past and may in the future attempt to recruit our employees. While our employees are required to sign standard agreements concerning confidentiality and ownership of inventions, we may not be able to prevent them from working with our competitors and providing their expertise to such companies, which could potentially harm our business.

We are dependent on a small number of distributors

We derive our sales primarily through indirect channels. During 2008, we derived approximately 50% of our sales from our 10 largest distributors, with the largest distributor accounting for approximately 16% of our sales, and the second largest distributor accounting for approximately 14% of our sales. During 2007, these two distributors accounted for approximately 30% of our sales.

We expect that a small number of distributors will continue to generate a significant portion of our sales. Furthermore, there has been an industry trend toward consolidation among our distributors, and we expect this trend to continue in the near future which could further increase our reliance on a small number of distributors for a significant portion of our sales. If these distributors reduce the amount of their purchases from us, our business, operating results and financial condition could be materially adversely affected.

Our future success is highly dependent upon our ability to establish and maintain successful relationships with our distributors. In addition, we rely on these entities to provide many of the training and support services for our products and equipment. Accordingly, our success depends in large part on the effective performance of these distributors. Recruiting and retaining qualified distributors and training them in our technology and products requires significant time and resources. Further, we have no long-term contracts or minimum purchase commitments with any of our distributors, and our contracts with these distributors do not prohibit them from offering products or services that compete with ours. Our competitors may be effective in providing incentives to existing and potential distributors to favor their products or to prevent or reduce sales of our products. Our distributors may choose not to offer our products exclusively or at all. Our failure to establish and maintain successful relationships with distributors would likely materially adversely affect our business, operating results and financial condition.

We purchase several key components and finished products from sole or limited sources, and we are increasingly dependent on contract manufacturers

Many components, subassemblies and modules necessary for the manufacture or integration of our products are obtained from a sole supplier or a limited group of suppliers. Our reliance on sole or limited suppliers, particularly foreign suppliers, and our reliance on subcontractors involves several risks, including a potential inability to obtain an adequate supply of required components, subassemblies or modules and reduced control over pricing, quality and timely delivery of components, subassemblies or modules. While we expend resources to qualify additional component sources, consolidation of suppliers in the industry and the small number of viable alternatives, have limited the results of these efforts.

Managing our supplier and contractor relationships is particularly difficult during time periods in which we introduce new products and during time periods in which demand for our products is increasing, especially if demand increases more quickly than we expect.

Difficulties in managing relationships with current contract manufacturers could impede our ability to meet the demand for our products and adversely affect our operating results.

We are dependent on a limited number of product families

Currently, we derive most of our revenues from sales of Internet security products primarily under our VPN-1, UTM-1, Power-1 and related brands, as well as related revenues from software updates, maintenance and other services. We expect this to continue to be the case in the foreseeable future. Following the acquisition of Protect Data, we also began to generate revenue from data security products and associated software updates, maintenance and support services. Our future growth depends heavily on our ability to effectively develop and sell new and acquired products as well as add new features to existing products. For more details, see Item 4 Information on Check Point and Item 5 Operating and Financial Review and Prospects.

We incorporate third party technology in our products, which may make us dependent on the providers of these technologies and expose us to potential intellectual property claims.

Our products contain certain technology that others license to us. Third party developers or owners of technologies may not be willing to enter into, or renew, license agreements with us regarding technologies that we may wish to incorporate in our products, either on acceptable terms or at all. If we cannot obtain licenses to these technologies, we may be at a disadvantage compared with our competitors who are able to license these technologies. In addition, when we do obtain licenses to third party technologies that we did not develop, we may have little or no ability to determine in advance whether the technology infringes the intellectual property rights of others. Our suppliers and licensors may not be required or may not be able to indemnify us in the event that a claim of infringement is asserted against us, or they may be required to indemnify us only up to a maximum amount, above which we would be responsible for any further costs or damages.

We incorporate open source technology in our products which may expose us to liability and have a material impact on our product development and sales

Some of our products utilize open source technologies. These technologies are licensed to us on varying license structures, including the General Public License. This license and others like it pose a potential risk to products in the event they are inappropriately integrated. In the event that we have not, or do not in the future, properly integrate software that is subject to such licenses into our products, we may be required to disclose our own source code to the public, which could enable our competitors to eliminate any technological advantage that our products may have over theirs. Any such requirement to disclose our source code or other confidential information related to our products could materially adversely affect our competitive position and impact our business results of operations and financial condition.

We are the defendants in various lawsuits and are also subject to certain tax disputes and governmental proceedings, which could adversely affect our business, results of operations and financial condition

We operate our business in various countries, and accordingly attempt to utilize an efficient operating model to optimize our tax payments based on the laws in the countries in which we operate. This can cause disputes between us and various tax authorities in different parts of the world.

In particular, following audits of our 2002 and 2003 corporate tax returns, the Israeli Tax Authority (the ITA) issued orders challenging our positions on several issues, including matters such as the usage of funds earned by our approved enterprise for investments outside of Israel, deductibility of employee stock options expenses, percentage of foreign ownership of our shares, taxation of interest earned outside of Israel and deductibility of research and development expenses. The largest amount in dispute relates to the treatment of investment income on cash that is held and managed by our wholly-owned Singapore subsidiary, which the ITA is seeking to tax in Israel. In an additional challenge to this amount, the ITA reclassified the transfer of funds from Check Point to our subsidiary in Singapore as a dividend for purposes of the Law for the Encouragement of Capital Investments, which would result in tax on the funds transferred. The ITA orders also contest our positions on various other issues. The ITA, therefore, demanded the payment of additional taxes in the aggregate amount of NIS 963 million with respect to 2002 (assessment received on December 27, 2007) and NIS 151 million with respect to 2003 (assessment received on May 29, 2008), in each

case including interest as of the assessment date. We have appealed the orders relating to both years with the Tel-Aviv District Court, and these appeals are pending. See also Item 8 Financial Information under the caption Legal Proceedings. There can be no assurance that the ITA will accept our positions on these matters or others and, in such an event, we may record additional tax expenses if these matters are settled for amounts in excess of our current provisions.

We have also been named as a defendant in a lawsuit filed by Information Protection and Authentication of Texas, LLC in the Eastern District of Texas on December 30, 2008. The plaintiff s original complaint in the lawsuit alleges infringement by us of U.S. patents nos. 5,311,591 and 5,412,717 and seeks an injunction and an unspecified amount of damages. We currently intend to vigorously defend against plaintiff s claims, but cannot assure you of the outcome of this litigation.

We are currently engaged in various legal disputes with two minority shareholders of our subsidiary SofaWare Technologies Ltd. One of these shareholders is alleging we are oppressing him as a minority shareholder, and he is seeking to compel us to purchase his shares. He is currently valuing his shares at NIS 16 million, subject to change. The other minority shareholder claims that he and other minority shareholders are entitled to exercise veto rights with respect to certain actions of SofaWare. The same shareholder also filed a derivative claim against us on behalf of SofaWare. On February 14, 2008, the court partially accepted the derivative claim and ordered that we pay SofaWare NIS 13 million plus interest. Both parties have appealed this ruling. We are also engaged in additional litigation with these two minority shareholders. We believe that the claims filed by these two minority shareholders are without merit and intend to contest these claims vigorously.

Further, we are the defendants in various lawsuits, including employment-related litigation claims, lease termination claims, patent infringement and other legal proceedings in the normal course of our business. Litigation and governmental proceedings can be expensive, lengthy and disruptive to normal business operations, and can require extensive management attention and resources, regardless of their merit. While we intend to defend the aforementioned matters vigorously, we cannot predict the results of complex legal proceedings, and an unfavorable resolution of a lawsuit or proceeding could materially adversely affect our business, results of operations and financial condition.

Class action litigation due to stock price volatility or other factors could cause us to incur substantial costs and divert our management s attention and resources

In the past, following periods of volatility in the market price of a public company s securities, securities class action litigation has often been instituted against that company. Companies such as ours in the software industry, and other technology industries, are particularly vulnerable to this kind of litigation as a result of the volatility of their stock prices. We have been named in the past as a defendant in this type of litigation in the past. Any litigation of this sort could result in substantial costs and a diversion of management s attention and resources.

We may not be able to successfully protect our intellectual property rights

We seek to protect our proprietary technology by relying on a combination of statutory as well as common law copyright and trademark laws, trade secrets, confidentiality procedures, and contractual provisions as indicated below in the section entitled Proprietary Rights in Item 4 Information on Check Point. We have certain patents in the United States and in some other countries, as well as pending patent applications. We cannot guarantee that pending patent applications will be issued, either at all or within the scope of the patent claims that we have submitted. In addition, someone else may challenge our patents and these patents may be found invalid. Furthermore, others may develop technologies that are similar to or better than ours, or may work around any patents issued to us. Despite our efforts to protect our proprietary rights, others may copy aspects of our products or obtain and use information that we consider proprietary. Although we do not know the extent to which there is piracy of our software products, software piracy is a persistent problem. We try to police this type of activity, but it is difficult to do so effectively. In addition, the laws of some foreign countries do not protect our proprietary rights to the same extent as the laws of the United States, Israel or Sweden. Our efforts to protect our proprietary rights may not be adequate and our competitors may independently develop technology that is similar to our technology. If we are unable to secure, protect, and enforce our intellectual property rights, such failure could harm our brand and adversely impact our business, financial condition, and results of operations.

If a third-party asserts that we are infringing its intellectual property, whether successful or not, it could subject us to costly and time-consuming litigation or expensive licenses, which could harm our business

There is considerable patent and other intellectual property development activity in our industry. Our success depends, in part, upon our ability not to infringe upon the intellectual property rights of others. Our competitors, as well as a number of other entities and individuals, own or claim to own intellectual property relating to our industry. From time to time, third parties may claim that we are infringing upon their intellectual property rights, and we may be found to be infringing upon such rights. As noted above, we have been named as a defendant in a lawsuit filed by Information Protection and Authentication of Texas, LLC in the Eastern District of Texas on December 30, 2008. The plaintiff s original complaint in the lawsuit alleges infringement by us of U.S. patents nos. 5,311,591 and 5,412,717 and seeks an injunction and

an unspecified amount of damages. In addition, third-parties have in the past sent us correspondence regarding their intellectual property and in the future we may receive claims that our products infringe or violate their intellectual property rights. Furthermore, we may be unaware of the intellectual property rights of others that may cover some or all of our technology or products. Any claims or litigation could cause us to incur significant expenses and, if successfully asserted against us, could require that we pay substantial damages or royalty payments, prevent us from selling our products, or require that we comply with other unfavorable terms. In addition, we may decide to pay substantial settlement costs and/or licensing fees in connection with any claim or litigation, whether or not successfully asserted against us. Even if we were to prevail, any litigation regarding our intellectual property could be costly and time-consuming and divert the attention of our management and key personnel from our business operations. As such, third-party claims with respect to intellectual property may increase our cost of goods sold or reduce the sales of our products, and may have a material and adverse effect on our business.

We are exposed to various legal, business, political and economic risks associated with international operations; these risks could increase our costs, reduce future growth opportunities and affect our results of operations

We sell our products worldwide, and we book a significant portion of our revenue outside the United States. We intend to continue to expand our international operations, which will require significant management attention and financial resources. In order to continue to expand worldwide, we will need to establish additional operations, hire additional personnel and recruit additional channel partners, internationally. To the extent that we are unable to do so effectively, our growth is likely to be limited and our business, operating results and financial condition may be materially adversely affected.

Our international revenues and operations subject us to many potential risks inherent in international business activities, including, but not limited to:

- Technology import and export license requirements.
- Costs of localizing our products for foreign countries, and the lack of acceptance of localized products in foreign countries.
- Trade restrictions.
- Imposition of or increases in tariffs or other payments on our revenues in these markets.
- Changes in regulatory requirements.
- Greater difficulty in protecting intellectual property.
- Difficulties in managing our overseas subsidiaries and our international operations.
- Declines in general economic conditions.
- Political instability and civil unrest which could discourage investment and complicate our dealings with governments.
- Variety of foreign laws and legal standards.
- Expropriation and confiscation of assets and facilities.
- Difficulties in collecting receivables from foreign entities or delayed revenue recognition.
- Differing labor standards.
- Potentially adverse tax consequences, including taxation of a portion of our revenues at higher rates than the tax rate that applies to us in Israel.
- Fluctuations in currency exchange rates and the impact of such fluctuations on our results of operations and financial position.
- The introduction of exchange controls and other restrictions by foreign governments.

These difficulties could cause our revenues to decline, increase our costs or both. This is also specifically tied to currency exchange rates which has an impact on our financial statements based on currency rate fluctuations.

We are controlled by a small number of shareholders who may make decisions with which you or others may disagree

As of December 31, 2008, our directors and executive officers owned approximately 20.7% of the voting power of our outstanding ordinary shares, or 25.4% of our outstanding ordinary shares if the percentage includes options currently exercisable or exercisable within 60 days of December 31, 2008 (the exercise price of some of these options is greater than our current share market price). The interests of these shareholders may differ from your interests and present a conflict. If these shareholders act together, they could exercise significant influence over our operations and business strategy. For example, although these shareholders hold considerably less than a majority of our outstanding ordinary shares, they may have sufficient voting power to influence matters requiring approval by our shareholders, including the election and removal of directors and the approval or rejection of mergers or other business combination transactions. In addition, this concentration of ownership may delay, prevent or deter a change in control, or deprive a shareholder of a possible premium for its ordinary shares as part of a sale of our company.

We may be required to indemnify our directors and officers in certain circumstances

We have entered into agreements with each of our directors and senior officers to insure, indemnify and exculpate them against some types of claims, subject to dollar limits and other limitations. Subject to Israeli law, these agreements provide that we will indemnify each of these directors and senior officers for any of the following liabilities or expenses that they may incur due to an act performed or failure to act in their capacity as our director or senior officer:

- Monetary liability imposed on the director or senior officer in favor of a third party in a judgment, including a settlement or an arbitral award confirmed by a court.

- Reasonable legal costs, including attorneys fees, expended by a director or senior officer as a result of an investigation or proceeding instituted against the director or senior officer by a competent authority; provided, however, that such investigation or proceeding concludes without the filing of an indictment against the director or senior officer and either:

  No financial liability was imposed on the director or senior officer in lieu of criminal proceedings, or

  Financial liability was imposed on the director or senior officer in lieu of criminal proceedings, but the alleged criminal offense does not require proof of criminal intent.

- Reasonable legal costs, including attorneys fees, expended by the director or senior officer or for which the director or senior officer is charged by a court:

  In an action brought against the director or senior officer by us, on our behalf or on behalf of a third party,

  In a criminal action in which the director or senior officer is found innocent, or

  In a criminal action in which the director or senior officer is convicted, but in which proof of criminal intent is not required.

We Face the Risk of a Decrease in Our Cash Balances and Losses in Our Investment Portfolio

Investment income is an important component of our net income. The ability to achieve our investment objectives is affected by many factors, some of which are beyond our control. We rely on third-party money managers to manage the majority of our investment portfolio in a risk-controlled framework. Our cash throughout the world is invested in fixed-income securities and is affected by changes in interest rates. Interest rates are highly sensitive to many factors, including governmental monetary policies and domestic and international economic and political conditions.

The outlook for our investment income is dependent on the future direction of interest rates, the amount of any share repurchases or acquisitions that we effect and the amount of cash flows from operations that are available for investment. Any significant decline in our investment income or the value of our investments as a result of falling interest rates, deterioration in the credit of the securities in which we have invested, or general market conditions, could have an adverse effect on our results of operations and financial condition.

The current global credit crisis may significantly decrease the value of our investment assets

The performance of the capital markets affects the values of funds that are held in marketable securities. These assets are subject to market fluctuations and will yield uncertain returns, which may fall below our projected return rates. Due to recent market developments, including a series of rating agency downgrades, the fair value of these investments may decline. During 2008, we recorded an other-than-temporary impairment of marketable securities in the amount of $11.2 million in accordance with SFAS 115. Check Point expects that market conditions will continue to fluctuate and that the fair value of our investments may be impacted accordingly.

Our cash, cash equivalents, short-term deposit and marketable securities totaled $1,443.8 million as of December 31, 2008. Our investment portfolio policy is buy and hold, while minimizing credit risk by setting maximum concentration limit per issuer and credit rating. Our investments consist primarily of government and corporate debentures. Although we believe that we generally adhere to conservative investment guidelines, the continuing turmoil in the financial markets may result in impairments of the carrying value of our investment assets. We classify our investments as available-for-sale. Changes in the fair value of investments classified as available-for-sale are not recognized to income during the period, but rather are recognized as a separate component of equity until realized. Realized losses in our investments portfolio may adversely affect our financial position and results. Had we reported all the changes in the fair values of our investments into income, our reported net income for the year ended December 31, 2008, would have decreased by $5.9 million.

One of our primary market risk exposures is changes in interest rates, which relates primarily to our investments in marketable securities. A decline in market interest rates, such as the significant global decline in recent months, has had an adverse effect on our investment income. In a declining interest rate environment, borrowers may seek to refinance their borrowings at lower rates and, accordingly, prepay or redeem securities we hold more quickly than we initially expected. This action may cause us to reinvest the redeemed proceeds in lower yielding investments. An increase in market interest rates could also have an adverse effect on the value of our investment portfolio, for example, by decreasing the fair values of the fixed income securities that comprise a substantial majority of our investment portfolio.

Our business and operations are subject to the risks of earthquakes and other natural catastrophic events

Our headquarters in the United States, as well as certain of our research and development operations, are located in the Silicon Valley area of Northern California, a region known for seismic activity. A significant natural disaster, such as an earthquake, could damage our operations and properties, and adversely affect our business, operating results, and financial condition.

Risks Related to Our Operations in Israel

Potential political, economic and military instability in Israel, where our principal executive offices and our principal research and development facilities are located, may adversely affect our results of operations

We are incorporated under the laws of the State of Israel, and our principal executive offices and principal research and development facilities are located in Israel. Accordingly, political, economic and military conditions in and surrounding Israel may directly affect our business. Since the State of Israel was established in 1948, a number of armed conflicts have occurred between Israel and its Arab neighbors. Any hostilities involving Israel or the interruption or curtailment of trade between Israel and its present trading partners, or a significant downturn in the economic or financial condition of Israel, could materially adversely affect our operations. Since October 2000, terrorist violence in Israel has increased significantly. In recent years, there has been an escalation in violence among Israel, Hamas, Hezbollah, the Palestinian Authority and other groups, including the recent extensive hostilities along Israel s border with Gaza in December 2008 and January 2009. Ongoing and revived hostilities or other Israeli political or economic factors could materially adversely affect our business, operating results and financial condition.

The tax benefits available to us require us to meet several conditions, and may be terminated or reduced in the future, which would increase our taxes.

For the year ended December 31, 2008, our effective tax rate was 16%. There can be no assurance that our effective tax rate will not change over time as a result of changes in corporate income tax rates, changes in the tax laws of the various countries in which we operate and fluctuations in the growth rate of our business. We have benefited or currently benefit from a variety of government programs and tax benefits that generally carry conditions that we must meet in order to be eligible to obtain any benefit.

If we fail to meet the conditions upon which certain favorable tax treatment is based, we would not be able to claim future tax benefits and could be required to refund tax benefits already received. Additionally, some of these programs and the related tax benefits are available to us for a limited number of years, and these benefits expire from time to time.

Any of the following could have a material effect on our overall effective tax rate:

- Some programs may be discontinued,
- We may be unable to meet the requirements for continuing to qualify for some programs,
- These programs and tax benefits may be unavailable at their current levels,
- Upon expiration of a particular benefit, we may not be eligible to participate in a new program or qualify for a new tax benefit that would offset the loss of the expiring tax benefit, or
- We may be required to refund previously recognized tax benefits if we are found to be in violation of the stipulated conditions.

Additional details are provided in Item 5 Operating and Financial Review and Products under the caption Taxes on income , in Item 10 Additional Information under the caption Israeli taxation, foreign exchange regulation and investment programs , and in notes 10b and 11 to our consolidated financial statements.

Our operations may be disrupted by the obligations of our personnel to perform military service

Many of our officers and employees in Israel are obligated to perform military reserve duty until they reach age 45 and, in the event of a military conflict, could be called to active duty. Our operations could be disrupted by the absence of a significant number of our employees related to military service or the absence for extended periods of military service of one or more of our key employees. Military service requirements for our employees could materially adversely affect our business, operating results and financial condition.

Provisions of Israeli law and our articles of association may delay, prevent or make difficult an acquisition of us, prevent a change of control, and negatively impact our share price

Israeli corporate law regulates acquisitions of shares through tender offers and mergers, requires special approvals for transactions involving directors, officers or significant shareholders, and regulates other matters that may be relevant to these types of transactions. Furthermore, Israeli tax considerations may make potential acquisition transactions unappealing to us or to some of our shareholders. For example, Israeli tax law may subject a shareholder who exchanges his or her ordinary shares for shares in a foreign corporation, to taxation before disposition of the investment in the foreign corporation. These provisions of Israeli law may delay, prevent or make difficult an acquisition of our company, which could prevent a change of control and, therefore, depress the price of our shares.

In addition, our articles of association contain certain provisions that may make it more difficult to acquire us, such as the provision which provides that our board of directors may issue preferred shares. These provisions may have the effect of delaying or deterring a change in control of us, thereby limiting the opportunity for shareholders to receive a premium for their shares and possibly affecting the price that some investors are willing to pay for our securities.

Additional details are provided in Item 10 Additional Information under the caption Articles of association and Israeli Companies Law Anti-takeover measures.

Our operations expose us to risks associated with fluctuations in foreign currency exchange rates that could adversely affect our business

Although we have operations throughout the world, the majority of our revenue and approximately 56% of our operating costs in 2008 were denominated in, or linked to, the U.S. dollar. Accordingly, we consider the U.S. dollar to be our functional currency. However, approximately 44% of our operating costs in 2008 were incurred in other currencies, particularly in Israeli Shekels, Euros, Swedish Krona and British Pounds. During 2007 and 2008, the Israel shekel appreciated against the U.S. dollar, which resulted in a significant increase in the U.S. dollar cost of our operations in Israel. As a result of this differential, from time to time we may experience increases in the costs of our operations outside the United States, as expressed in dollars, which could have a material adverse effect on our results of operations and financial condition.

The imposition of exchange or price controls or other restrictions on the conversion of foreign currencies could also have a material adverse effect on our business, results of operations and financial condition.

ITEM 4. INFORMATION ON CHECK POINT

We develop, market and support a wide range of software and combined hardware and software products and services for information technology (IT) security and offer our customers an extensive portfolio of network and gateway security solutions, data and endpoint security solutions and management solutions. Our solutions operate under a unified security architecture that enables end-to-end security with a single line of unified security gateways and allow a single agent for all endpoint security that can be managed by a single unified management console. This unified management allows for ease of deployment and centralized control and is supported and enforced with real-time security updates. Our products and services are sold to enterprises, service providers, small and medium sized businesses and consumers. Our Open Platform for Security (OPSEC) framework allows customers to extend the capabilities of our products and services with third-party hardware and security software applications. Our products are sold, integrated and serviced by a network of partners worldwide.

In January 2007, we completed the acquisition of Protect Data AB (Protect Data), which was a public company listed on the Stockholm Stock Exchange, and completed the integration of Protect Data into Check Point s business. Protect Data operates its business through its wholly owned subsidiary, Pointsec Mobile Technologies AB, a worldwide provider of mobile data protection. Pointsec delivers solutions for automatic data encryption that keeps sensitive information stored on mobile computing devices, such as laptops, PDAs, smartphones and removable media (e.g., USB devices), confidential and secure. With the acquisition of Protect Data, Check Point entered into the data security market.

On December 22, 2008, we entered into an Asset Purchase Agreement with Nokia to acquire its security appliance business. The pending acquisition is expected to close in the first or second quarter of 2009 and is subject to regulatory approvals and customary closing conditions. Check Point has collaborated with Nokia s security appliance business over the past decade to deliver industry-leading enterprise security solutions. Upon completion of the acquisition, Check Point intends to build on this collaboration to provide an extended security appliance portfolio developed, manufactured and supported by Check Point. Additional details regarding the important events in the development of our business since the beginning of 2008 are provided in Item 5 Operating and Financial Review and Prospects under the caption Overview.

We were incorporated as a company under the laws of the State of Israel in 1993 under the name of Check Point Software Technologies Ltd. Our registered office and principal place of business is located at 5 Ha Solelim Street, Tel Aviv 67897 Israel. The telephone number of our registered office is 972-3-753-4555. Our company s Web site is www.checkpoint.com. The contents of our Web site are not incorporated by reference into this Annual Report on Form 20-F.

This Annual Report on Form 20-F is available on our Web site. If you would like to receive a printed copy via mail, please contact our Investor Relations department at 800 Bridge Parkway, Redwood City, CA 94065, U.S.A., tel: 650-628-2050, email: ir@us.checkpoint.com.

Our agent for service of process in the United States is CT Corporation System, 818 West Seventh Street, Los Angeles, CA 90017 U.S.A., tel: 213-627-8252.

Industry Background

The ability to access and distribute information is a key strategic asset in today s competitive business environment. The resulting need to effectively use and communicate information as well as work more collaboratively has led to the extensive deployment of network-based communication systems delivering connectivity. Increased connectivity has in turn expanded the need for technology to safeguard and manage the access to information available over these networks and to secure information contained on these connected systems.

Increase in connectivity

Over the past decade, global connectivity has continued to increase rapidly. The emergence of increased reliance on the Internet for business communications and transactions increases the need for secured access to information and applications and raises challenges associated with providing it. Companies of all sizes in most industries are embracing and supporting increased connectivity for mobile and remote employees. This includes connectivity to corporate data and application resources, as well as general Internet access. Remote users are increasingly able to access private corporate networks and information from a growing spectrum of mobile devices, including laptops, PDAs, smartphones, portable media players, and removable media storage devices. The expansion of network access to mobile workers and the increase in information contained on mobile devices is driving demand to secure all devices with access to corporate information.

These developments and the need for secure and managed communications have led to nearly universal adoption of Virtual Private Networks (VPNs). VPNs enable a secured exchange of private information over networks, including the Internet. Sharing information and utilizing services are now widely available, both within the enterprise, and with business partners and customers. As a result, businesses are able to share internal information and to run enterprise applications across geographically dispersed facilities, as well as enable customers, suppliers and other business partners to link into their enterprise information systems. These connectivity services include access to Web information, messaging applications, such as email, database access, transaction-processing services, voice-over-IP services and video teleconferencing services.

The need for network and gateway security

The use of networks within organizations and the use of the Internet by organizations of all sizes have increased the risk that information technology resources can be attacked. Organizations have recognized this risk and are deploying security solutions in an effort to protect their information and infrastructure from damage and unauthorized access.

The primary means of controlling access to organizational networks and protecting against attacks is the deployment of Internet firewalls. Firewalls are typically deployed at the demarcation of an organization s Local Area Network (LAN) and the Internet or within an organization between different segments and are used to strictly control traffic into and out of the organizational network or between segments. Firewall technology is constantly evolving to detect and defeat highly sophisticated network and application-level attacks that are increasingly prevalent on the Internet today. Organizations are also deploying an additional layer of security by applying security software to networked endpoint devices, such as personal computers. Endpoint security includes personal firewall, security and policy enforcement features that have been specifically designed for internal and remote personal computing devices. In addition to protecting their IT assets from attack, organizations have taken steps to guard their sensitive information traversing untrusted networks, such as the Internet. Securing organizational information on the Internet is critical as organizations utilize the Internet as their corporate network backbone to link company offices and employees. Transmitting information over the Internet without adequate security exposes this information to unauthorized interception, manipulation or replication. To mitigate this risk, organizations have deployed VPNs to encrypt and authenticate their Internet traffic.

Firewalls and VPNs are usually integrated as a single product. Unified Threat Management (UTM) solutions integrate firewalls and VPNs with additional security features, such as network intrusion prevention and virus scanning in a single, centrally managed security solution. Integrating multiple security functionalities delivers greater security for all network traffic and facilitates efficient management and enforcement of an organization s security policies.

IT security administrators within organizations have primarily focused on securing the network perimeter. However, organizations are realizing the importance of also securing their internal networks and Web-based business applications. Many of today s security threats and attacks emerge within organizations. Internal security breaches can be in the form of worm outbreaks and other attacks that are introduced through mobile and wireless devices, internal hacking and misuse of business applications by users within an organization. In addition, due to the rapid development of Web-based technologies and the increased reliance on the Web to connect remote users, Web-based applications and protocols are highly vulnerable to attacks. This presents many security challenges for businesses because internal networks and Web-based communications contain unique complexities, such as programming code embedded in the network traffic and communications protocols that are used in these environments. Security solutions, for both internal and Web security, need to incorporate an understanding of the applications and protocols that are common in these environments.

The need for data and endpoint security increases as workers continue to move away from centralized corporate environments. While network security offers effective solutions for data in motion, sensitive data can still be lost or accessed improperly. Organizations are deploying an additional layer of security by applying security software to endpoint devices, such as personal computers. Endpoint security includes personal-firewall, Network Access Control (NAC), program control, antivirus, anti-spyware, data security, URL filtering, anti-spam and remote

access features that have been specifically designed for remote personal computing devices.

Lost or stolen computers can end up in the wrong hands, intentionally or unintentionally. Companies of all sizes and government agencies face the consequences of losing sensitive data from lost laptop computers, removable media or plug-and-play storage devices. This drives the need for a complete data protection solution that secures data on all common platforms, deploys easily, scales to any size organization and meets strict compliance requirements related to privacy laws and regulations. For example, a number of publicized cases involving large corporations losing unencrypted laptops and exposing millions of customers and employees to potential identity theft have prompted a surge in data protection legislation and regulatory compliance laws worldwide. The relative ease with which data may be lost makes data security a major concern for organizations. To mitigate this risk, organizations are looking to extend security beyond the network infrastructure, to the data itself.

The primary means of protecting data that resides on endpoints are as follows: full-disk encryption of the hard drive with access control (rendering the data useless to unauthorized parties); media encryption and port protection (to prevent unauthorized copying of sensitive data to USB flash drives, writable CDs and DVDs, etc.); and mobile device and memory card data encryption (to prevent sensitive data from being accessed on lost or stolen PDAs and smartphones).

Products and Services

Our products, services and technologies provide the following protection:

1. Network security gateway

Our wide range of network security gateways allows our customers to implement their security policies on network traffic between internal networks and the Internet as well as between internal networks and private networks used with partners. These gateways are available as either appliances or software solutions providing customers with a broad range of deployment options, including the ability to customize the configuration to best meet their security needs. Our security gateways include the following technologies to secure traffic and optimize performance:

- Firewall Inspects traffic as it passes through security gateways, classifying it based on various criteria such as source and destination of connection, protocol, services and application used. This provides a means to allow, block and log each connection based on the organization s security policy. Our firewall technology is based on several key differentiated technologies, including:

  Patented Stateful Inspection technology that allows flexible and programmable classification of network traffic.

  Application Intelligence technology that contains various means to detect the correct use of application protocols and can block attacks that attempt to utilize such exploits in specific applications.

  Network Address Translation Allows hiding of internal addresses so internal users are not exposed to external threats, as well as connecting private networks that use generic addresses using publicly defined external addresses.

  Specific technologies to prevent denial-of-service (DoS) attacks on networks. These attacks include various ways of overloading applications and networks in multiple requests that try to slow and stop their response.

- Intrusion Prevention Technologies Monitors the network for malicious or unwanted traffic and has the ability to detect and block known attacks on the network or system based on usage patterns as well as unknown attacks based on out of bounds usage of certain services and protocols. Intrusion prevention technology is supported by online security update services that provide the latest defense mechanisms including signatures for the most recent attacks. Intrusion prevention is available as technology integrated into the firewall or as a dedicated IPS system.

- Virtual Private Networks (VPNs) Provide the means to enable private communication over a network by encrypting traffic between various sub-networks (site-to-site) or individual computers (such as mobile computers) and the corporate network. This prevents exposing sensitive traffic and attempts to modify such communication and replicate certain transactions.

- Content Screening Enables screening of specific application protocols such as Web traffic to allow/block access to specific Web addresses based on their content. There is also screening for viruses (antivirus) to detect downloads of malicious applications.

- Messaging Security Prevents the use of the messaging infrastructure (such as email) to attack the organization. Six dimensions of messaging security technologies are available in our products, including prevention of emailed spam and the use of messaging protocols for various attacks, as well as enabling the scanning of email traffic for malware and viruses embedded in email.

- Web-Based Communications Allow remote and mobile employees to securely connect to their organizations networks via a Web browser (via Secure Sockets Layer VPN technology) and defend against attacks that target our customers Web-based business applications.

- Security Acceleration Patented security acceleration technologies speed up security inspection to ensure a high service level for business applications. These technologies improve overall throughput and reduce latency through several different techniques, such as load balancing and load sharing between physical gateways, balancing security traffic loads between multiple cores on multi-core processors, and offloading repetitive decisions from the general-purpose processor to specialized hardware and software.

- Virtualization Certain Check Point gateways are available on a virtual security operations platform that enables organizations to consolidate multiple security gateways in a single hardware system and to secure virtual server environments.

2. Data and endpoint security

Our data and endpoint security technologies provide multiple technologies that run on individual computers (endpoints) connecting to the network, such as desktop computers, mobile computers and communications devices. These technologies include:

- Personal Firewall Prevents network attacks on individual computers by blocking internal attacks and the proliferation of network worms within the corporate network, as well as attacks on home and mobile computers that are connected to public networks. Our personal firewall technologies include proprietary technologies such as:

  Inbound and Outbound Firewalls Prevent malware and Trojan horses not only from attacking individual computers but also from sending data out through unauthorized applications.

  Program Advisor and Operating System Firewall Using a real-time network service, we can detect malicious and/or unauthorized applications running on individual computers and block their activities.

  Network Access Control Provides the network with information on the compliance of individual computers to the organization s security policy and allows selective connectivity of devices to the network based on their compliance.

- Data Protection Data stored on individual endpoint devices can be exposed to unauthorized parties by copying it to external devices, or even more commonly, if devices fall into the wrong hands. Lost and stolen computers provide unauthorized parties the chance to access all the information stored on these computer hard drives. We protect against these risks to data through:

  Full-Disk Encryption All the data stored on an individual PC can be fully encrypted, so that unauthorized parties cannot read this data even if they get physical access to the disk drive.

  Port Control Allows an organization to prevent or control the transfer of information from individual computers to external devices such as USB memory devices and external hard drives.

  Media Encryption Enables encryption of data stored on mobile devices, such as CDs and DVDs and other external removable media.

- Remote Access VPNs Enable mobile devices to securely access an organization s network by encrypting all traffic between mobile devices and the corporate network and ensure mobile devices and users are properly authenticated.

- Anti-Malware Antivirus, anti-spyware and other technologies detect viruses and other malware that try to run on any device and/or circumvent its operation. Our anti-malware technology uses some of the industry s best engines and operates on-demand when a new application is stored or retrieved from the device or the network and by scanning computers against this type of attack.

The four technologies above are consolidated into a single endpoint security agent managed by a single administrative console. This is the industry s first and only such solution. It provides total security at the endpoint and eliminates the need to deploy and manage multiple agents, reducing complexity, conflicts between various security components, procurement and management costs and the total cost of ownership.

3. Security management

A key element in implementing the above security technologies is the ability to effectively manage the deployment while ensuring consistent operations in accordance with organization policy. Our strategy is to provide a single console for security management. This single console reduces the need for multiple, sometimes conflicting, management systems that require a high degree of specialization and training. The key aspects include:

- Centralized Policy Management Tools that allow the definition of various aspects of the security policy, such as network access rights, application controls, etc.
- Provisioning Tools Allow the daily deployment and removal of individual entities, such as new gateways, users and devices.
- Monitoring Tools Show the status of each controlled device and allow the immediate detection and remediation of various situations.
- Auditing Tools Consistent tools to log and monitor every change made to the security infrastructure and to ensure that all changes are accounted for and can be traced and tracked by company policies.
- Security Information and Event Management Today s complex, multi-layered security architecture consists of many devices to ensure servers, hosts and network applications are protected from harmful activity. These devices all generate voluminous logs that are difficult and time consuming to interpret. Our solutions automatically prioritize security events for decisive, intelligent action. Clear, graphical reports help inform decisions related to resource allocation, security optimization and regulatory compliance.

We package and market our products and services under different names and at a variety of prices. Each package addresses security tasks for different network environments and has corresponding support offerings.

Our management and gateway software products run in a variety of deployment environments and on platforms that include standard workstations, servers and dedicated appliances. Check Point has both software and dedicated appliance solutions for both gateway and management products. Additional appliance solutions are also available from our partners such as Nokia Corporation, Crossbeam Systems Inc. and International Business Machines Corporation (IBM). Different client products run on different client Operating Systems (OS), such as Microsoft Windows, Mac OS, Microsoft Windows Mobile, Symbian, Linux and PalmOS.

Moving Forward

In February 2009, Check Point introduced a new architecture aimed at changing the way customers deploy their IT security infrastructure: the Software Blade architecture. Security environments of large, medium and small companies are becoming more complex as they attempt to address continually evolving threats with new protections. Each new protection requires a new product, hardware platform, management console and set of daily events to monitor. Corporations security has become increasingly complex and incurs increased operational expenses in order to implement and support these incremental additions to the existing security infrastructure.

As described above in our product and service offerings, in response to rising IT operational expenses, organizations began to seek consolidated security devices that incorporated several functions into a single device, such as unified threat management (UTM) appliance. UTM devices consolidate firewall, VPN, intrusion prevention, antivirus and other functions in a single, turnkey solution and have

been successful in helping companies reduce capital and operational expenditures. Although clearly a good solution to date, it cannot keep up with the rapidly evolving threat environment which requires that UTM functionality be extended.

In an effort to simultaneously address the need for scalable security solutions and the retention of initial investments, Check Point introduced the Software Blade architecture, which provides customers with the ability to tailor their security gateways based on their specific needs at any time. Check Point Software Blade architecture offers businesses a common platform to deploy independent, modular and interoperable security applications or software blades , such as firewall, virtual private network (VPN), intrusion prevention system (IPS), anti-virus, policy management or security reporting blades. The new architecture allows customers to select the exact security software blades they need and to combine them into a single, centrally managed solution. With the new Software Blade architecture customers will be able to move functionality from one system to another, consolidate or split functionalities between systems and assure performance for each software blade by setting usage thresholds. All of these capabilities are intended to enable customers to scale their security needs while simultaneously optimizing their security costs.

Check Point s Software Blade architecture

Check Point s Software Blade architecture delivers extensible, flexible and manageable security solutions to companies of all sizes. The Software Blade architecture provides customers with the flexibility to custom configure Check Point security gateways and security management systems to meet their specific needs. Customers can deploy any combination of security functions by either purchasing pre-defined systems or building a fully customized solution by choosing a Software Blade container and selecting from a library of over 20 software blades. Each blade runs a separate security function. Therefore, customers can easily extend their security solutions by adding new blades without the necessity of purchasing separate systems. Check Point s Software Blade architecture enables organizations to deploy security dynamically, as needed, with lower total cost of ownership, full integration of the various security functions and with central management of the security system.

Technologies

We have developed and acquired a variety of technologies that secure networks and information. Our products and services implement these technologies to protect our customers networks and private information, enabling their IT administrators to define and enforce their security policies across the network. These technologies also collect and bring together related information, monitor security and traffic flow, and analyze and update configurations to reflect changes in the security policy.

Stateful Inspection technology

Our patented Stateful Inspection technology is a de facto standard in network security technology. In order to provide accurate and highly efficient traffic inspection, Stateful Inspection extracts and maintains extensive state information, i.e., data that provides context for future screening decisions, from all relevant communication layers.

Stateful Inspection runs on a network gateway or an endpoint, such as a personal computer, and enables the screening of all data attempting to pass from one network to another. By tracking each connection, the system ensures that data passing through the gateway complies with a defined security and traffic policy, traffic is managed according to priority, and security decisions are made in an intelligent and timely manner.

Stateful Inspection enables our products to inspect network traffic at high speed. This means that as network traffic increases, our products respond efficiently to the larger volumes of data. Our Stateful Inspection technology can be adapted to new protocols, software applications, and security threats. It can be upgraded and can be run on a wide range of operating systems.

Application Intelligence

Our Application Intelligence technology provides a set of advanced capabilities that prevents the exploitation of vulnerabilities in business applications, including vulnerabilities in the application code, communication protocols, and the underlying operating system. Application Intelligence provides security for these applications by running multiple security checks, including validation of compliance to standards, validation of expected use of protocols, inspection for known malicious content and control of application layer operations. The result is the ability to proactively shield applications from attack without relying on specific attack signatures. We have integrated our Application Intelligence technology into our Power-1, UTM-1, UTM-1 Edge, VPN-1 Power, UTM, Safe@Office, IPS-1, Connectra, and VPN-1 Power VSX products.

Security Management Architecture (SMART)

Security Management Architecture (SMART), a core component of our unified security architecture, enables our customers to configure and manage security policies from a central administrative point. SMART enables the definition and ongoing management of security policies for businesses of all sizes. This object-oriented architecture maps real-world entities, such as networks and users, to graphical representations that can be manipulated in a database. Integrated monitoring and reporting tools improve the manageability of the system by providing administrators with real-time information on the state of network and security systems. These tools also provide longer term trending information that is useful for periodic security management tasks, such as security audits.

Security and network traffic enforcement technologies (based on Stateful Inspection)

Based on our Stateful Inspection technology, the INSPECT engine scans all incoming and outgoing traffic at security enforcement points. These are typically located at the network perimeter as security gateways, on critical servers or inside the network dividing the network into separate segments.

The INSPECT engine can perform a variety of functions on inspected network traffic as listed below:

- Drop it when the security policy has been violated.

- Encrypt it to create a secured VPN that enables the transfer of private data over public networks, such as the Internet.
- Prioritize it for Quality of Service (QoS), which is the ability of a network to provide better service for selected traffic.
- Send it for further processing, such as authentication, content inspection or the filtering of malicious or unwanted traffic.

We have developed a broad range of technologies that can be implemented by our INSPECT engine. In addition, third party technologies can be implemented through our Open Platform for Security (OPSEC) framework, which is described below.

SecurePlatform

SecurePlatform bundles the Check Point security solutions together with a prehardened operating system (OS), in a single package that is easy to deploy. It optimizes the performance of security and OSes and includes a set of tools that ease setup and network configuration, thus reducing the total cost of ownership for security gateways and security management servers. SecurePlatform runs on a variety of open systems, i.e., systems whose key interfaces are based on widely supported standards.

ClusterXL

Our ClusterXL technology provides high availability and load sharing to keep businesses running. It distributes traffic between clusters of redundant gateways so that the computing capacity of multiple machines may be combined to increase total throughput. If an individual gateway becomes unreachable, all connections are redirected to a designated backup without interruption. Integration with our management and enforcement points enables simple deployment.

CoreXL

CoreXL is a technology for intelligently balancing security traffic loads between multiple cores on multi-core processors. It results in a higher level of performance for integrated intrusion prevention. CoreXL, a Check Point security gateway running on a multi-core platform, can be configured to have a large number of active intrusion prevention settings, such as those that would be found protecting sensitive information or networks, while maintaining high performance levels.

SecureXL

SecureXL is a framework of software and hardware technologies, including third-party technologies, designed to increase performance. By using SecureXL, hardware vendors can accelerate the performance of appliances on which our software is installed. With SecureXL, our products can be integrated into high-performance networks typically found in large enterprises and service providers.

TrueVector technology

Our TrueVector technology is a patented, flexible and efficient software technology for enabling high-performance, scalable and robust Internet security for personal computers.

TrueVector stops attempts to send confidential data to unauthorized parties by malicious software, such as keystroke loggers and Trojan horses. It monitors all applications running on protected computers, allowing trusted applications to engage in network communications, while blocking network connections by untrusted applications. TrueVector enforces security policies that are centrally created and managed, stand alone or any combination of these. In addition, TrueVector may be configured to make protected computers invisible to external attackers. The technology is used in the Check Point Endpoint Security and ZoneAlar