COMMTOUCH SOFTWARE LTD
Form 20-F
March 29, 2012

UNITED STATES
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, 2011

OR

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

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 .

For the transition period from _____ to _____

Commission file number 000 26495

COMMTOUCH SOFTWARE LTD.

(Exact name of Registrant as specified in its charter and
translation of Registrant s name into English)

Israel
(Jurisdiction of incorporation or organization)

4A Hazoran Street
Poleg Industrial Park,
P.O. Box 8511
Netanya 42504, Israel
011 972 9 863 6888
(Address of principal executive offices)

Ron Ela, CFO, Fax: 011-972-9-8636863. Same address as above.
(Name, Telephone, Email 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 each exchange on which registered
Ordinary Shares, par value NIS 0.15 per share	**NASDAQ Capital 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 (December 31, 2011).

Ordinary Shares, par value NIS 0.15	24,093,617

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

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

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

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 has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). x Yes oNo

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

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

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

U.S. GAAP x	International Financial Reporting Standards as issued by the International Accounting Standards Board o	Other o

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

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.

Unless otherwise indicated, all references in this document to Commtouch, the Company, we, us or our are to Commtouch Software Ltd. and its wholly owned subsidiary, Commtouch Inc., as relating to consolidated financial information contained herein.

The selected consolidated statements of operations data for the years ended December 31, 2009, 2010 and 2011 and the selected consolidated balance sheet data as of December 31, 2010 and 2011 have been derived from the Consolidated Financial Statements of Commtouch included elsewhere in this report. The selected consolidated statements of operations data for the years ended December 31, 2007 and 2008 and the selected consolidated balance sheet data as of December 31, 2007, 2008 and 2009 have been derived from the Consolidated Financial Statements of Commtouch not included elsewhere in this report. Our historical results are not necessarily indicative of results to be expected for any future period. The data set forth below should be read in conjunction with Item 5. Operating and Financial Review and Prospects and the Consolidated Financial Statements and the Notes thereto included elsewhere herein:

	Year Ended December 31,				
	2007	2008	2009	2010	2011
	(USD in thousands, except per share data)				
Selected Data:					
Revenues	$ 11,250	$ 14,092	$ 15,189	$ 18,161	$ 23,016
Operating income	$ 1,610	$ 1,931	$ 2,696	$ 3,360	$ 3,308
Net income attributable to ordinary and equivalently participating shareholders	$ 2,109	$ 2,270	$ 5,160	$ 4,403	$ 4,598
Basic net earnings per share	$ 0.08	$ 0.09	$ 0.21	$ 0.19	$ 0.19
Diluted net earnings per share	$ 0.08	$ 0.08	$ 0.20	$ 0.18	$ 0.19
Weighted average number of shares used in computing basic net earnings per share	24,847	25,619	24,532	23,575	23,620
Weighted average number of shares used in computing diluted net earnings per share	27,591	26,929	25,292	24,874	24,654
Total Assets	$ 18,210	$ 20,709	$ 25,190	$ 31,982	$ 39,534

FORWARD LOOKING STATEMENTS

Except for the historical information contained in this Annual Report, the statements contained in this Annual Report are forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995, as amended, and other federal securities laws with respect to our business, financial condition and results of operations. Such forward-looking statements reflect our current view with respect to future events and financial results.

We urge you to consider that statements which use the terms anticipate, believe, expect, plan, intend, estimate and expressions are intended to identify forward-looking statements. We remind readers that forward-looking statements are merely predictions and therefore inherently subject to uncertainties and other factors and involve known and unknown risks that could cause the actual results, performance, levels of activity, or our achievements, or industry results, to be materially different from any future results, performance, levels of activity, or our achievements, or industry results, expressed or implied by such forward-looking statements. Such forward-looking statements appear in Item 4 Information on the Company and Item 5 Operating and Financial Review and Prospects, as well as elsewhere in this Annual Report. Readers

are cautioned not to place undue reliance on these forward-looking statements, which speak only as of the date hereof. Except as required by applicable law, including the securities laws of the United States, we undertake no obligation to update or revise any forward-looking statements to reflect new information, future events or circumstances, or otherwise after the date hereof. We have attempted to identify significant uncertainties and other factors affecting forward-looking statements in the Risk Factors section that appears below.

RISK FACTORS

You should carefully consider the following risk factors before you decide to buy our Ordinary Shares. You should also consider the other information in this report. If any of the following risks actually occur, our business, financial condition, operating results or cash flows could be materially adversely affected. This could cause the trading price of our Ordinary Shares to decline, and you could lose part or all of your investment. The risks described below are not the only ones facing us. Additional risks not presently known to us, or that we currently deem immaterial, may also impair our business operations.

Business Risks

If the market does not continue to respond favorably to our current Internet security solutions, including our anti-spam, Zero-Hour antivirus, Mail Reputation, Command Antivirus and Uniform Resource Locator or URL filtering solutions, or our future solutions do not gain acceptance, we will fail to generate sufficient revenues.

Our success depends on the continued acceptance and use of our Internet security solutions by current and new businesses, Original Equipment Manufacturers or OEM, and service provider customers. We have been selling our inbound anti-spam products (as a stand-alone product) for over eight years, Zero-Hour virus outbreak detection product for approximately seven years, our GlobalView Mail Reputation perimeter defense solution for approximately six years, our URL filtering solutions for over two years, our outbound spam solution for approximately two years and the Command Antivirus solution for over a year.

As the markets for messaging, antivirus and Web security products continue to mature and consolidate, we are seeing increasing competitive pressures and demands for even higher quality products at lower prices. This increasing demand comes at a time when Internet security threats are more varied and intensive, challenging even the top end solutions to keep their performance at an industry acceptable high level of accuracy. If our solutions do not continue to evolve to meet market demand, or newer products on the market prove more effective, our business could fail. Also, if growth in the markets for these solutions begins to slow, our business will suffer dramatically.

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

The crisis in the financial and credit markets that began in 2008 in the United States, and that led to a global economic slowdown, seems to have become more acute in certain countries of Europe that have been experiencing a sovereign debt crisis. If the economies of countries in which our customers and potential customers are located 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 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 OEM partners, 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 economic conditions in key markets do not improve or continue to improve, or revert to a recessionary state, our business, operating results and financial condition may be adversely impacted in a material way.

Tighter governmental enforcement of regulations could decrease the distribution of unsolicited bulk (spam) email and malicious software and decrease demand for our solutions, or increase our cost of doing business.

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) established a framework of U.S. administrative, civil, and criminal tools to combat spam. The law establishes both civil and criminal prohibitions to assist in deterring the most offensive forms of spam, including unmarked sexually-oriented messages and emails containing fraudulent headers. Under the law, senders of email are required to honor a request by a consumer not to receive any further unsolicited messages. While past high profile prosecutions of direct marketers seemingly have not had much of a deterrent effect on marketers of unsolicited email, it is not known whether or not future enforcement actions will prove effective.

In addition, various state legislatures have enacted laws aimed at regulating the distribution of unsolicited email. While we are not clear as to the reasons, in the past year we have begun to see a gradual decline in the amount of spam traffic on the Internet.

These and similar legal measures, both in the United States and worldwide, may have the effect of reducing the amount of unsolicited email and malicious software that is distributed and hence diminish the need for our Internet security solutions. Any such developments would have an adverse impact on our revenues.

We depend upon OEM partners, service providers and, to a lesser extent, resellers.

We expect to continue to be dependent upon OEM partners, service providers and resellers for a significant portion of our revenues, which will be derived from sales of our messaging, antivirus and Web security solutions. Our operating results and financial condition may be materially adversely affected if:

Anticipated orders or payments from these customers fail to materialize;

Some of the key customers cease the promotion of our business or begin to promote additional solutions in a layered approach to email defense, anti-malware and URL filtering management; or

Some of our key customers businesses fail as a result of a deepening global economic crisis.

Our quarterly operating results may fluctuate, which could adversely affect the value of your investment.

A number of factors, many of which are enumerated in this Risk Factors section, are likely to cause fluctuations in our operating results or cause our share price to decline. These factors include:

Our ability to successfully market our messaging, antivirus and Web security solutions in new markets, both domestic and international;

Our ability to successfully develop and market new, modified or upgraded solutions, as may be needed;

The continued acceptance of our solutions by our current customer base;

Our ability to expand our workforce with qualified personnel, as may be needed;

Unanticipated bugs or other problems affecting the delivery of our solutions to customers;

The success of our customers sales efforts to their customer base;

The solvency of our customers and their ability to allocate sufficient resources towards the marketing of our solutions;

Our customers ability to effectively integrate our solutions into their product offerings;

The substantial decrease in information technology spending;

The pricing of our solutions;

Our ability to timely collect fees owed by our customers;

A renewed global slowdown;

Sudden, dramatic fluctuations in exchange rates of currencies covering the fees we collect from our foreign customers versus the currencies utilized in our business (namely, the New Israeli Shekel, or NIS, the U.S. Dollar and Euro);

Our ability to add cost-effective space and equipment to our current detection centers, or Detection Centers, in a timely and effective manner to match the rate of growth in our business, plus our ability to build new, cost-effective detection centers as worldwide demand for our products may require; and

The effectiveness of our end user support, whether provided by our customers or directly by Commtouch.

Our products and services have changed many times since we commenced operations in 1991. For example, in September 2010, we acquired the Command Antivirus unit of Authentium, and have integrated this new business into our existing business. Future changes in our product offerings may require that we adjust our business processes and workforce, which can cause fluctuations in our results from operations.

We have many established competitors who are offering a multitude of solutions to the problems of spam/virus distribution and Web-related security threats.

The market for Internet security products remains intensely competitive and is subject to rapid changes in technology. We expect both product and pricing competitive pressures to increase in the future. Some of our competitors have longer operating histories, greater brand recognition, larger technical staffs and/or greater financial, technical and marketing resources, and other advantages compared to us. This competition could have a negative impact on our business and financial results. Additional details are provided in Item 4. Information on the Company.

Our ability to continue to increase our revenues will depend on our ability to successfully execute our sales and business development plan.

The complexity of the underlying technological base of messaging, antivirus and Web security solutions, and the current landscape of the markets, require highly trained sales and business development personnel to educate prospective resellers, OEM and service provider partners and customers regarding the use and benefits of our solutions. It may take time for our current and future employees to convey to potential, as well as current, OEM/service provider partners and resellers how to most effectively market and utilize our solutions. As a result, our sales and business development personnel may not be able to compete successfully against larger, more heavily financed and more experienced sales and business development departments of our competitors.

The loss of our key employees would adversely affect our ability to manage our business, therefore causing our operating results to suffer and the value of your investment to decline.

Our success depends on the skills, experience and performance of our senior management and other key personnel. The loss of the services of any of our senior management or other key personnel could materially and adversely affect our business. The loss of our software developers or senior operations personnel may also adversely affect the continued development and support of our messaging, antivirus and Web security solutions, thereby causing our operating results to suffer and the value of your investment to decline.

We do not have employment agreements inclusive of set periods of employment with any of our key personnel. We cannot prevent them from leaving at any time. We do not maintain key-person life insurance policies, listing us as a beneficiary, on any of our employees.

Our business and operating results could suffer if we do not successfully address potential risks inherent in doing business overseas.

As of December 31, 2011, we had sales offices in Israel and the United States. We also are marketing our messaging, antivirus and Web security solutions in international markets by utilizing appropriate distribution channels. However, we may not be able to compete effectively in international markets due to various risks inherent in conducting business internationally, such as:

Differing technology standards;

Inability of distribution channels to successfully market our solutions;

Export restrictions;

Difficulties in collecting accounts receivable and longer collection periods;

Unexpected changes in regulatory requirements;

Political and economic instability;

Potentially adverse tax consequences; and

Limited enforcement mechanisms for protecting intellectual property rights.

Any of these factors could adversely affect the Company s prospective international sales and, consequently, business and operating results.

Our Web security and antivirus solutions may be adversely affected if we are not able to receive sufficient components from third party suppliers. Our Web security and antivirus solutions rely in part on certain components supplied by third parties (separate third parties per each solution) pursuant to contractual relationships. If these third parties breach their agreements with us, we may have difficulty in securing alternative sources for these components in a timely manner and thus our Web security and antivirus solutions may not perform at the level we expect. If this were to occur, the effectiveness of these solutions would drop, they would become less attractive to customers/potential customers and anticipated revenues could decline.

Technology Risks

We may not have the resources or skills required to adapt to the changing technological requirements and shifting preferences of our customers and their users.

The messaging, antivirus and Web security industries are characterized by difficult technological challenges, sophisticated distributors of Internet security threats, multiple-variant viruses, unique phishing scams and constantly evolving malevolent software distribution practices and targets that could render our solutions and proprietary technology ineffective. Our success depends, in part, on our ability to continually enhance our existing messaging, antivirus and Web security solutions and to develop new solutions, functions and technology that address the potential needs of prospective and current customers and their users. The development of proprietary technology and necessary enhancements entails significant technical and business risks and requires substantial expenditures and lead-time. We may not be able to keep pace with the latest technological developments. We may not be able to use new technologies effectively or adapt to OEM, customer or end user requirements or emerging industry standards. Also, we must be able to act more quickly than our competition, and may not be able to do so.

Our solutions may be adversely affected by defects or denial of service attacks, which could cause our OEM partners, customers or end users to stop using our solutions.

Our messaging, antivirus and Web security solutions are based in part upon new and complex software and highly advanced computer systems. Complex software and computer systems can contain defects, particularly when first introduced or when new versions are released, and are possible targets for denial of service attacks instigated by hackers . Although we conduct extensive testing and implement Internet security processes, we may not discover defects to or vulnerabilities in our software or systems that affect our new or current solutions or enhancements until after they are delivered. Although we have not experienced any material defects or vulnerabilities to date in our messaging, antivirus and Web security offerings, it is possible that, despite testing by us, defects or vulnerabilities may exist in the solutions we provide. These defects or vulnerabilities could cause or lead to interruptions for customers of our solutions, resulting in damage to our reputation, legal risks, loss of revenue, delays in market acceptance and diversion of our development resources, any of which could cause our business to suffer.

Our messaging, antivirus and Web security solutions may be adversely affected if we are not able to receive a sufficient sampling of Internet traffic or our Detection Centers were to become unavailable.

Our messaging, antivirus and Web security solutions are dependent, in part, on the ability of our Detection Centers to analyze, in an automated fashion, live feeds of Internet and Web related traffic received through our services to customers and other contractual arrangements. If we were to suffer an unanticipated, substantial decrease in such traffic or our multiple Detection Centers become unavailable for any significant period, the effectiveness of our technologies would drop, our product offerings would become less attractive to customers/potential customers and revenues could decline.

Our Command Antivirus offering remains relatively new for us, and we still may not fully appreciate the needs of customers and risks inherent in this new market.

Our acquisition of the Command Antivirus business from Authentium in September 2010 represented our first efforts at expansion into the antivirus market. While we hired the core team of ex-Authentium employees and contractors who possess the expertise to manage the Command Antivirus business and, to date, the integration of this business has been successful, nevertheless we cannot be totally certain that we have anticipated all possible issues that might arise with our cloud computing technology infrastructure and this offering. Should unanticipated issues arise, sales of our antivirus solution likely will slow and our business will suffer.

For example, because of the complexity of the antivirus products, we understand that in the past, errors were found in versions of these products that were not detected before first introduced, or appeared in new versions or enhancements, and we may find such errors in the future. Failures, errors or defects in our antivirus products could result in security breaches or compliance violations for our customers, disruption or damage to their networks or other negative consequences and could result in negative publicity, damage to our reputation, declining sales, increased expenses and customer relation issues. Such failures could also result in product liability damage claims against us by our customers, even though our agreements with our customers typically contain provisions designed to limit our exposure to potential product liability claims.

The antivirus products have in the past, and may at times in the future, falsely detect viruses or computer threats that do not actually exist. These false alarms, while typical in the security industry, would likely impair the perceived reliability of our products and may therefore adversely impact market acceptance of our antivirus products.

Investment Risks

Our directors, executive officers and principal shareholders will be able to exert significant influence over matters requiring shareholder approval and could delay or prevent a change of control. [Disclose if the company is aware of a shareholders agreement between the main shareholder and other major shareholders or the directors & officers]

Our directors and affiliates of our directors, our executive officers and our shareholders who currently individually beneficially own over five percent of the voting power in the Company (together known as affiliated entities), beneficially own, in the aggregate, approximately 32.8% of our outstanding Ordinary Shares as of December 31, 2011. Included in the calculation of voting power are options exercisable by the affiliated entities within 60 days thereof (with some having an exercise price greater than the market price of our shares as of December 31, 2011). If they vote together (especially if they were to exercise all vested options into shares entitled to voting rights in the Company), these shareholders will be able to exercise significant influence over all matters requiring shareholder approval, including the election of directors and approval of significant corporate transactions. In this regard, we know of no shareholders or voting agreement between major shareholders or between such shareholders and directors or officers.

This concentration of ownership could also delay or prevent a change in control of Commtouch. In addition, conflicts of interest may arise as a consequence of the significant shareholders control relationship with us, including:

- Conflicts between significant shareholders, and our other shareholders whose interests may differ with respect to, among other things, our strategic direction or significant corporate transactions;
- Conflicts related to corporate opportunities that could be pursued by us, on the one hand, or by these shareholders, on the other hand; or
- Conflicts related to existing or new contractual relationships between us, on the one hand, and these shareholders, on the other hand.

Our Ordinary Shares are traded on more than one market and this may result in price variations.

Our Ordinary Shares are traded primarily on the NASDAQ Capital Market and also on the Tel Aviv Stock Exchange. Trading in our Ordinary Shares on these markets is made in different currencies (U.S. dollars on the NASDAQ Capital Market, and NIS, on the Tel Aviv Stock Exchange), and at different times (resulting from different time zones, different trading days and different public holidays in the United States and Israel). Consequently, the trading prices of our Ordinary Shares on these two markets often differ. Any decrease in the trading price of our Ordinary Shares on one of these markets could cause a decrease in the trading price of our Ordinary Shares on the other market.

If we will be in need of additional capital, we may not be able to secure additional funds on acceptable terms, or at all, and the Company s business could suffer.

We have invested heavily in technology development and an acquisition. We expect to continue to spend financial and other resources on developing, acquiring and introducing new offerings and maintaining our corporate organizations and strategic relationships. We also expect to invest resources in research and development projects to further enhance our solutions.

Notwithstanding the Company s current, solid financial condition, should additional funding become necessary we may be unable to secure capital on acceptable terms, or at all, due to, among other things, difficulties in the capital and credit markets. In such case, the Company s business could suffer.

Intellectual Property Risks

If we fail to adequately protect our intellectual property rights or face a claim of intellectual property infringement by a third party, we could lose our intellectual property rights or be liable for significant damages.

We regard our patented and patent pending technology, copyrights, service marks, trademarks, trade secrets and similar intellectual property as critical to our success, and rely on patent, trademark and copyright law, trade secret protection and confidentiality or license agreements with our employees and customers to protect our proprietary rights. See Item 4. Information on the Company, *Intellectual Property* for information pertaining to our patent activities. We may seek to patent certain additional software or other technology in the future. Any such patent applications might not result in patents issued within the scope of the claims we seek, or at all.

Despite our precautions, unauthorized third parties may copy certain portions of our technology, reverse engineer or obtain and use information that we regard as proprietary or otherwise infringe or misappropriate our patent or our patent pending technology, trade secrets, copyrights, trademarks and similar proprietary rights. In addition, the laws of some foreign countries do not protect proprietary rights to the same extent as do the laws of the United States. Thus, our means of protecting our proprietary rights in the United States or abroad, as well as our financial resources, may not be adequate, and competitors may independently develop similar technology.

We cannot be certain that our Internet security solutions do not infringe issued patents in certain parts of the world. Therefore, other parties, whether in the United States or elsewhere, may assert infringement claims against us. We may also be subject to legal proceedings and claims from time to time in the ordinary course of our business, including claims of alleged infringement of copyrights, trademarks and other intellectual property rights of third parties by ourselves and our customers. Our customer agreements typically include indemnity provisions, so we may be obligated to defend against third party intellectual property rights infringement claims on behalf of our customers. Such claims, even if not meritorious, could result in the expenditure of significant financial and managerial resources. We may not have the proper resources in order to adequately defend against such claims. During 2011, one such indemnification demand was made by a customer, and we continue to cooperate with that customer in seeking to defeat the underlying patent infringement claims. While we believe that adequate non-infringement and/or invalidity arguments exist, it is too early in the proceedings to anticipate the outcome of this matter.

Risks Relating to Operations in Israel

We have important facilities and resources located in Israel, which has historically experienced military and political unrest.

We are incorporated under the laws of the State of Israel. Our principal research and development facilities are located in Israel. Although the majority of our past sales were made to customers outside Israel, we are nonetheless directly influenced by the political, economic and military conditions affecting Israel. Any major hostilities involving Israel, or the interruption or curtailment of trade between Israel and its present trading partners, could significantly harm our business, operating results and financial condition.

Since the State of Israel was established in 1948, a number of armed conflicts have occurred between Israel and its Arab neighbors. Recent years have witnessed extensive hostilities from time to time along Israel s northern and southern borders, which resulted in missiles being fired from Lebanon and the Gaza Strip into Israel. Ongoing and revived hostilities or other Israeli political or economic factors could harm our operations and cause our revenues to decrease.

Recent uprisings in various countries in the Middle East and North Africa are affecting the political stability of those countries. This instability in the region may lead to deterioration of the political and trade relationships that exist between the State of Israel and certain of these and other countries. In addition, this instability may affect the global economy and marketplace, including as a result of increases in oil and gas prices. In addition, Israel and some companies doing business with Israel have been the subject of an economic boycott by Arab countries and their close allies since Israel s establishment.

The regional instability and restrictive laws and policies described above may have an adverse impact on our operating results, financial condition and expansion of our business.

Our results of operations may be negatively affected by the obligation of key personnel to perform military service.

Certain of our officers and employees are currently obligated to perform annual reserve duty in the Israel Defense Forces and are subject to being called for active military duty at any time in the event of a national emergency, such as in connection with the hostilities along Israel s border with the Gaza Strip in December 2008 and January 2009. Although Commtouch has operated effectively under these requirements since its inception, we cannot predict the effect of these obligations on Commtouch in the future. Our operations could be disrupted by the absence for a significant period of one or more of our officers or key employees due to military service. Any disruption in our operations would harm our business.

Because a substantial portion of our revenues historically have been generated in U.S. dollars and the Euro, and a significant portion of our expenses have been incurred in NIS, our results of operations may be adversely affected by currency fluctuations.

We have generated a substantial portion of our revenues in U.S. dollars and Euro, and incurred a portion of our expenses, principally salaries and related personnel expenses in Israel, in NIS. We anticipate that a significant portion of our expenses will continue to be denominated in NIS. As a result, we are exposed to risk to the extent that the value of the U.S. dollar decreases against the NIS and the Euro. In that event, the U.S. dollar cost of our operations will increase and our U.S. dollar-measured results of operations will be adversely affected, as occurred during a portion of 2011, when the NIS and the Euro appreciated against the U.S. dollar, which resulted in a significant increase in the U.S. dollar cost of our operational expenses and revenues. We cannot predict the trend for future years. Our operations also could be adversely affected if we are unable to guard against currency fluctuations in the future. To date, we have not engaged in any significant hedging transactions. In the future, we may enter into currency hedging transactions to decrease the risk of financial exposure from fluctuations in the exchange rate of the dollar against the NIS. Foreign currency fluctuations, and our attempts to mitigate the risks caused by such fluctuations, could have a material and adverse effect on our results of operations and financial condition.

The government programs and benefits which we previously received require us to meet several conditions and may be terminated or reduced in the future.

Prior to 1998, we received grants from the Government of Israel, through the Office of the Chief Scientist of the Israeli Ministry of Industry, Trade & Labor, or OCS, for the financing of a significant portion of our research and development expenditures in Israel. These grants totaled $0.6 million. Subsequently, in 2001, we received $0.6 million and in 2002 we received $0.2 million. We did not submit an application for funding during the period 2004 2008. In 2009 and 2010, our applications for funding were approved in the amounts of approximately $0.5 million and $0.6 million respectively. We again did not submit an application during 2011 and the first quarter of 2012 and we do not expect to receive any grants during 2012.

In order to meet specified conditions in connection with previous grants and programs of the OCS, we have made representations to the Israel government about our Israeli operations. From time to time the conduct of our Israeli operations has deviated from our forecasts. If we fail to meet the conditions of the grants, including the maintenance of a material presence in Israel, or if there is any material deviation from the representations made by us to the Israeli government, we could be required to refund the grants previously received (together with an adjustment based on the Israeli consumer price index and an interest factor) and would likely be ineligible to receive OCS grants in the future.

Under the Law for the Encouragement of Industrial Research and Development, 5744-1984 and the related regulations, the discretionary approval of an OCS committee is required for any transfer of technology developed with OCS funding, including in the context of certain acquisitions of companies that have received OCS funding, or for the transfer of manufacturing rights outside of Israel. OCS approval is not required for the export of any products resulting

from the research and development. There is no assurance that we will receive the required approvals for any proposed future transfer. Such approvals, if granted, may be subject to the following additional restrictions:

- a requirement to pay the OCS a portion of the consideration we receive upon any sale of such technology to an entity that is not Israeli. The scope of the support received, the royalties that were paid by us, the amount of time that elapsed between the date on which the know-how was transferred and the date on which the grants were received, as well as the sale price, will be taken into account in order to calculate the amount of the payment; and

- the transfer of manufacturing rights could be conditioned upon an increase in the royalty rate and payment of increased aggregate royalties (up to 300% of the amount of the grant plus interest, depending on the percentage of the manufacturing that is foreign).

These restrictions may impair our ability to sell certain of our older technology assets outside of Israel. The restrictions will continue to apply even after we repay the full amount of royalties payable for the grants.

You may have difficulties enforcing a U.S. judgment against us and our executive officers and directors or asserting U.S. securities laws claims in Israel.

We are organized under the laws of Israel, and we maintain significant operations in Israel. In addition, the majority of our directors and executive officers are not residents of the United States and most of their assets and our assets are located outside the United States. Service of process upon our non-U.S. resident directors or executive officers and enforcement of judgments obtained in the United States against us and our directors and executive officers may be difficult to obtain within the United States. It may be difficult to assert U.S. securities law claims in original actions instituted in Israel. Israeli courts may refuse to hear a claim based on a violation of U.S. securities laws because Israel is not the most appropriate forum in which to bring such a claim. In addition, even if an Israeli court agrees to hear a claim, it may determine that Israeli law and not U.S. law is applicable to the claim. If U.S. law is found to be applicable, the substance of the applicable U.S. law must be proved as a fact, which can be a time-consuming and costly process. Certain matters of procedure will also be governed by Israeli law. Furthermore, there is little binding case law in Israel addressing these matters.

Israeli courts might not enforce judgments rendered outside Israel which may make it difficult to collect on judgments rendered against us. Subject to certain time limitations, an Israeli court may declare a foreign civil judgment enforceable only if it finds that (a) the judgment was rendered by a court which was, according to the laws of the state of the court, competent to render the judgment; (b) the judgment may no longer be appealed; (c) the obligation imposed by the judgment is enforceable according to the rules relating to the enforceability of judgments in Israel and the substance of the judgment is not contrary to public policy; and (d) the judgment is executory in the state in which it was given.

Even if these conditions are satisfied, an Israeli court will not enforce a foreign judgment if it was given in a state whose laws do not provide for the enforcement of judgments of Israeli courts (subject to exceptional cases) or if its enforcement is likely to prejudice the sovereignty or security of the State of Israel. An Israeli court also will not declare a foreign judgment enforceable if (i) the judgment was obtained by fraud; (ii) there is a finding of lack of due process; (iii) the judgment was rendered by a court not competent to render it according to the laws of private international law in Israel; (iv) the judgment is at variance with another judgment that was given in the same matter between the same parties and that is still valid; or (v) at the time the action was brought in the foreign court, a suit in the same matter and between the same parties was pending before a court or tribunal in Israel.

Provisions of Israeli law may delay, prevent or make difficult an acquisition of Commtouch, which could prevent a change of control and therefore depress the price of our shares.

Israeli corporate law regulates mergers and acquisitions of shares through tender offers, requires special approvals for transactions involving significant shareholders and regulates other matters that may be relevant to these types of transactions. Furthermore, Israeli tax law treats stock-for-stock acquisitions between an Israeli company and a foreign company less favorably than does U.S. tax law. For example, Israeli tax law may subject a shareholder who exchanges his Ordinary Shares for shares in a foreign corporation to immediate taxation or to taxation before his investment in the foreign corporation becomes liquid. These provisions may adversely affect the price of our shares.

As a foreign private issuer whose shares are listed on the NASDAQ Capital Market, we may follow certain home country corporate governance practices instead of certain NASDAQ requirements.

As a foreign private issuer whose shares are listed on the NASDAQ Capital Market, we are permitted to follow certain home country corporate governance practices instead of certain requirements of the NASDAQ Listing Rules.

Among other things, we may follow home country practice with regard to composition of the board of directors and quorum at shareholders meetings. In addition, we may follow our home country law, instead of the NASDAQ Listing Rules, which require that we obtain shareholder approval for certain dilutive events, such as for the establishment or amendment of certain equity based compensation plans, an issuance that will result in a change of control of the Company, certain transactions other than a public offering involving issuances of a 20% or more interest in the Company and certain acquisitions of the stock or assets of another company.

A foreign private issuer that elects to follow a home country practice instead of NASDAQ requirements, must submit to NASDAQ in advance a written statement from an independent counsel in such issuer s home country certifying that the issuer s practices are not prohibited by the home country s laws. In addition, a foreign private issuer must disclose in its annual reports filed with the Securities and Exchange Commission or on its website each such requirement that it does not follow and describe the home country practice followed by the issuer instead of any such requirement (see Item 16G. Corporate Governance for a list of those home country practices followed by us). Accordingly, our shareholders may not be afforded the same protection as provided under NASDAQ s corporate governance rules.

Item 4. Information on the Company.

Overview

The legal name of the Company is Commtouch Software Ltd., and its principal executive offices are located at 4A Hazoran Street, Poleg Industrial Park, P.O.Box 8511, Netanya 42504, Israel, where our telephone number is 011 972 9 863 6888. The Company was incorporated as a private company under the laws of the State of Israel on February 10, 1991 and its legal form is a company limited by shares. Commtouch became a public company on July 15, 1999. Its Amended and Restated Articles of Association are on file in Israel with the office of the Israeli Registrar of Companies and available for public inspection at that office. The Company s wholly owned subsidiary, Commtouch Inc., has its principal office located at 292 Gibraltar Drive, Suite 107, Sunnyvale, California 94089, where our telephone number is (650) 864 2000, as well as another office located at 7121 Fairway Dr., St. 104, Palm Beach Gardens, FL 33418, tel: 561 575-3200. Commtouch Inc. is also in the process of opening a formal office in the Washington, D.C. area at 7927 Jones Branch Drive, Suite 2250, Tysons Corner, VA, where certain members of management and related personnel are to be located.

We are a provider of messaging, antivirus and Web security solutions to a wide array of customers and OEM and service provider distribution partners, including real-time Inbound Anti-Spam, Outbound Spam Protection for service providers, Zero-Hour virus outbreak protection and GlobalView Mail Reputation services, as well as Command Antivirus and GlobalView URL Filtering services. The Company offers its solutions to network and security vendors offering content security gateways, unified threat management, or UTM, solutions, network routers and appliances, antivirus solutions and to service providers such as Software-as-a-Service, or SaaS, vendors, Web hosting providers and Internet service providers. Our multiple services are intended to provide Internet security for various users of the Internet against the harmful effects of spam, malevolent software or malware , unwelcome websites, etc.

Additional Detail on Our Offerings

Our above-described services are typically accessed by our OEM and service provider customers through the integration of a Software Development Kit, or SDK, which, upon integration, is then able to communicate with our remote, worldwide Detection Centers in order to provide our customers and their users with the most up to date protection against the latest Internet threats that they are facing.

At the core of our messaging security offerings is our proprietary Recurrent Pattern Detection (RPD) technology which, in general terms, analyzes messages associated with mass email outbreaks and directs the blocking of such

emails, without the need to analyze individual messages. Outbound Spam Protection is intended to enable service providers to block emails being sent from their system that contain spam, phishing or malware, and identify the source of the problem. Inbound Anti-Spam is intended to enable customers to block their end users receipt of such unwanted emails. GlobalView Mail Reputation fights unwanted email at a network s perimeter, i.e. fighting them at the entry point, before these messages enter the network, based on identifying characteristics of the source of the email.

At the core of our Web security solutions is its in the cloud infrastructure, which analyzes various feeds from worldwide sources as well as data from our RPD pertaining to URLs, and provides a classification of the URLs based on a set of categories.

At the core of our Command Antivirus solutions is our proprietary detection and remediation technology and unique engine design based on a combination of heuristics, emulation and several types of signatures, as well as an in the cloud infrastructure, which allows for a high degree of flexibility for our OEM customers.

In February 2011, we announced the availability of all three of our principal service offerings messaging, antivirus and Web security in one unified SDK. The unified SDK can be integrated into the products of security and networking vendors on an OEM basis, as well as into service providers infrastructure. Typical solutions that would benefit from the unified engine are software or hardware solutions or services that combine multiple security technologies, such as UTM, secure content filtering gateways and SaaS security solutions. The three principal service offerings messaging, antivirus and Web security are still available also in non-unified, individual SDKs for our OEM and service provider customers.

We also offer the following services typically through reseller channels:

An enterprise anti-spam and Zero-Hour virus outbreak detection solution, which allows the reseller s customers to download an Enterprise Gateway (a software program) enabling the subject Commtouch services to be provided in real time by our Detection Centers. Through the Enterprise Gateway, messages are filtered at the customer organization s entry point, before being distributed to recipients, with added user-level controls and a top level of secure spam and virus detection services from the Detection Center, all allowing for real-time reaction to worldwide attacks.

Command Anti-Malware service known as CSAM , which offer world-class anti-malware protection for consumers and small businesses, as well as enterprises with hundreds of managed endpoints.

Sales and Marketing

We utilize third party distribution channels to sell our products. Generally, our software is provided to OEM and service provider customers, who in turn integrate the software into their product or service offerings for sale or provision of our services to their customers. We are paid service fees under a variety of fee structures, including fixed fee and fee sharing arrangements.

Our enterprise anti-spam and Zero-Hour anti-virus gateway services, as well as CSAM service, are sold through resellers, who pay us pre-negotiated fees after each sale is closed with a reseller s customer.

All Company sales are managed by the Company s and its U.S. subsidiary s business development/sales departments, each of which consists of a department head and a relatively small number of business development/sales professionals. The Company s marketing efforts are aimed mainly at potential OEM and service provider customers. The marketing department is concentrated in the Company s Israel office, though our personnel travel internationally in furtherance of the Company s marketing goals.

Intellectual Property

We regard our patented and patent pending anti spam and anti-virus technology, copyrights, service marks, trademarks, trade secrets and similar intellectual property as critical to our success, and rely on patent, trademark and copyright law, trade secret protection and confidentiality and/or license agreements with our employees, customers, partners and others to protect our proprietary rights.

During 2004, we purchased a United States patent, U.S. Patent No. 6,330,590. During 2005, we filed in the United States an anti-spam related patent application, claiming priority for a prior period based on the filing of U.S. Provisional Patent Application. This application remains outstanding. During 2006, we filed in the United States a

patent application relating to the prevention of spam in streaming systems or, in other words, unwanted conversational media sessions (i.e. voice and video related). This provisional application was converted to a formal patent application and, effective December 7, 2010, the United States Patent and Trademark Office split our application into three pending applications and issued us a new patent under the original application United States Patent No. 7,849,186. In 2011, a divisional patent was issued in connection with one of those split applications United States Patent No. 7,991,919, which will have a term concurrent with US Patent No. 7,849,186. During 2008, we filed a U.S. Provisional Patent Application for anti-malware data center aggregate, which was subsequently converted into a formal patent application and then rejected by the United States Patent and Trademark Office in 2011. We may seek to patent certain additional software or other technology in the future.

We are actively maintaining our registered trademark for COMMTOUCH , which is registered in the U.S., Canada, Israel, European Union and China. With the acquisition of certain assets of Authentium during 2010, we also acquired registered trademarks in Command Antivirus , Command Anti-Malware , Command On Demand , Command Interceptor and Galileo , as well as registered service marks in Authentium Authentium ESP . We are allowing the registration of Command Interceptor to lapse. A previous registration of PRONTO in Canada is still in force, but we are not maintaining this registration and it will lapse in 2014. Since at least September 2003, we have claimed trademark rights in RPD and Recurrent Pattern Detection , as applicable to our messaging security solutions. We have also been claiming trademark rights in Zero-Hour in relation to our virus outbreak detection product (and more recently one of our web security products) and GlobalView in relation to our intellectual property, or IP, reputation and Web security products, as well as our cloud computing network infrastructure.

It may be possible for unauthorized third parties to copy or reverse engineer certain portions of our products or obtain and use information that we regard as proprietary. In addition, the laws of some foreign countries do not protect proprietary rights to the same extent as do the laws of the United States. There can be no assurance that our means of protecting our proprietary rights in the United States or abroad will be adequate or that competing companies will not independently develop similar technology.

Other parties may assert infringement claims against us. We may also be subject to legal proceedings and claims from time to time in the ordinary course of our business, including claims of alleged infringement by us and/or our customers of the trademarks and other intellectual property rights of third parties. Our customer agreements typically include indemnity provisions, so we may be obligated to defend against third party intellectual property rights infringement claims on behalf of our customers. Such claims, even if not meritorious, could result in the expenditure of significant financial and managerial resources. During 2011, one such indemnification demand was made by a customer, and we continue to cooperate with that customer in seeking to defeat the underlying patent infringement claims. While we believe that adequate non-infringement and/or invalidity arguments exist, it is too early in the proceedings to anticipate the outcome of this matter.

Government Regulation

Laws aimed at curtailing the spread of spam have been adopted by the United States federal government, i.e. CAN-SPAM Act, and some individual U.S. states, with the CAN-SPAM Act superseding some state laws or certain elements thereof. See also disclosure under Item 3. Key Information Risk Factors Business Risks Tighter governmental enforcement of regulations could decrease the distribution of unsolicited bulk (spam) email and malicious software and decrease demand for our solutions, or increase our cost of doing business. Though not totally clear as to the exact reason, in the past year we have begun to see a gradual decline in the amount of spam traffic on the Internet. The continuation of this trend can have a negative effect our business, as potential customers may not view the need to acquire a robust anti-spam solution (i.e. in place of a legacy solution) with as much urgency.

The propagation of email viruses, whether through email or Web sites, which are aimed at destroying or stealing third party data, is illegal under standard state and federal law outlawing theft, misappropriation, conversion, etc., without the need for special legislation prohibiting such activities on the Internet. Despite the existence of these laws, sources for Internet viruses continue to spread multi-variant viruses seemingly without much fear of recrimination. New laws providing for more stringent penalties could be adopted in various jurisdictions, but it is unclear what, if any, affect these would have on the anti-virus industry in general and our Command Antivirus, Zero-Hour Virus Outbreak Detection and GlobalView URL filtering solutions in particular.

Employees

As of December 31, 2011, 2010 and 2009, we had 86, 93 and 72 employees, respectively, with all of them located in the United States and Israel. None of our U.S. employees are covered by a collective bargaining agreement. As of December 31, 2011, our employees were categorized as follows:

LOCATION	General & Administrative	Sales & Marketing	Research & Development	Hosting (Operations)	TOTAL:
ISRAEL OFFICE	8	13	31	-	52
U.S. OFFICE:					
California	4	6	-	8	18
Florida	3	1	10	-	14
Virginia	2	-	-	-	2

We believe that our relations with our employees are good.

Israeli law and certain provisions of the nationwide collective bargaining agreements between the Histadrut (General Federation of Labor in Israel) and the Coordinating Bureau of Economic Organizations (the Israeli federation of employers organizations) apply to Commtouch s Israeli employees. These provisions principally concern the maximum length of the workday and workweek, minimum wages, contributions to a pension fund, insurance for work related accidents, procedures for dismissing employees, determination of severance pay and other conditions of employment. Furthermore, pursuant to such provisions, the wages of most of Commtouch s Israeli employees are subject to cost of living adjustments, based on changes in the Israeli Consumer Price Index. The amounts and frequency of such adjustments are modified from time to time. Also, all Israeli employees employed for at least a year commencing in 2009 are entitled to the funding of pension benefits by preset monthly contributions of the employee and the employer. Israeli law generally requires the payment of severance pay upon the retirement or death of an employee or upon termination of employment by the employer or, in certain circumstances, by the employee. We currently fund our ongoing severance obligations by making monthly payments for insurance policies and by an accrual. A general practice in Israel followed by Commtouch, although not legally required, is the contribution of funds on behalf of certain employees to an individual insurance policy known as Managers Insurance. This policy provides a combination of savings plan, insurance and severance pay benefits to the insured employee. It provides for payments to the employee upon retirement or death and secures a substantial portion of the severance pay, if any, to which the employee is legally entitled upon termination of employment. Each participating employee contributes an amount equal to 5% of such employee s base salary, and the employer contributes between 13.3% and 15.8% of the employee s base salary. Full time employees who are not insured in this way are entitled to a savings account, to which each of the employee and the employer makes a monthly contribution of 5% of the employee s base salary. We also provide certain Israeli employees with an Education Fund, to which each participating employee contributes an amount equal to 2.5% of such employee s base salary, and the employer contributes an amount equal to 7.5% of the employee s base salary, up to a certain maximum base salary set by law.

Description of Property

All of our facilities are leased. Our headquarters, in Netanya, Israel, is approximately 1,057 square meters, and it houses senior management, research and development, sales, marketing and administrative personnel. Our subsidiary s Sunnyvale, California office, which is approximately 4,527 square feet in size, houses administrative, sales and hosting (operations) personnel; its office in Florida (approximately 3,000 square feet), houses the Command Antivirus operations and research and development personnel, plus a small number of administrative and sales personnel; and its office in Virginia is expected to house some management, administrative and sales related personnel (approximately 3,000 square feet).

Geographic Information

The Company conducts its business on the basis of one reportable segment in accordance with Accounting Standards Codification , or ASC, 280, Segment Reporting .

Revenues for Last Three Financial Years

See Item 5. Operating and Financial Review and Prospects Revenue Sources and the financial statements included elsewhere in this annual report. Below is a breakdown of our revenues by location (in thousands):

	Year December 31,		
	2009	**2010**	**2011**
Israel	$ 1,544	$ 2,047	$ 2,044
North America	8,032	9,184	12,655
Europe	3,776	4,454	4,869
Asia	1,508	1,976	3,036
Other	329	500	412
	$ 15,189	$ 18,161	$ 23,016

We have had only negligible capital expenditures and divestitures in the last three financial years.

Competitive Landscape

The markets in which Commtouch competes are intensely competitive and rapidly changing. However, we believe there are very few competitors that offer the complete package of anti-spam, anti-virus (both traditional and complementary real-time offerings), IP reputation and Web security protections that Commtouch provides.

The principal competitive factors in our industry include price, product functionality, product integration, platform coverage and ability to scale, worldwide sales infrastructure and global technical support. Some of our competitors have greater financial, technical, sales, marketing and other resources than we do, as well as greater name recognition and a larger installed customer base. Additionally, some of these competitors have research and development capabilities that may allow them to develop new or improved products that may compete with product lines we market and distribute, possibly at a lower cost. Our success will depend on our ability to adapt to these competing forces, to develop more advanced products more rapidly and less expensively than our competitors and/or to purchase new products by way of strategic acquisitions, and to educate potential customers as to the benefits of using our products rather than developing their own products.

In the market for messaging security solutions, there are sophisticated offerings that compete with our solutions. Email defense providers offering forms of software (gateway), multi-functional appliances and managed service solutions and which may be viewed as both competitors and potential customers to Commtouch include Symantec (Brightmail), TrendMicro, Intel (McAfee) and Cisco (IronPort). Messaging security providers offering solutions on an OEM basis similar to Commtouch s business model, and which may be viewed as direct competitors, include Cloudmark, Mailshell and Vade Retro.

Commtouch s GlobalView Mail Reputation Service competes in an evolving market. This market includes some established vendors, including TrendMicro, that are offering reputation-based solutions. In some cases, while the product positioning may be new, the underlying solutions may be mature for example, Spamhaus repositioning its RBL, or Real-time Block List, service as a commercial reputation service. In addition, there are several startups competing in this space.

The market for real-time virus protection products is also constantly evolving, as those promoting the proliferation of viruses continually seek new distribution techniques. Commtouch s real-time offering differs from traditional anti-virus solutions (such as our Command Antimalware solution) in that we offer an additional, complementary solution to signature and heuristic-based anti-virus engines. For this reason, our Zero-Hour virus outbreak protection engine has been employed by several security companies.

In the market for antimalware solutions, there a