CYREN Ltd.
Form 20-F
April 30, 2014

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

FORM 20–F

oREGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR (g) OF THE SECURITIES EXCHANGE ACT OF 1934

OR

xANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 for the fiscal year ended December 31, 2013

OR

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

OR

oSHELL 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

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

Israel
(Jurisdiction of incorporation or organization)

1 Sapir Road

5th Floor, Beit Ampa
P.O. Box 4014
Herzliya 46140, Israel
011–972–9–863–6888

(Address of principal executive offices)

Sue Lee, Esq., General Counsel, 7925 Jones Branch Drive, Suite 5200, McLean, VA 22102, Fax: 703-842-8227

(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, 2013).

Ordinary Shares, par value NIS 0.15 26,472,963

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

(APPLICABLE ONLY TO ISSUERS INVOLVED IN BANKRUPTCY PROCEEDINGS DURING THE PAST FIVE YEARS)

Indicate by check mark whether the registrant has filed all documents and reports required to be filed by Sections 12, 13 or 15(d) of the Securities Exchange Act of 1934 subsequent to the distribution of securities under a plan confirmed by a court.

Yes o No o

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 "CYREN", "the Company," "we," "us" or "our" are to CYRE Ltd., formerly known as Commtouch Software Ltd. and its consolidated subsidiaries, namely CYREN Inc., formerly known as Commtouch Inc., CYREN Iceland hf, formerly known as Commtouch Icelandhf, and CYREN Gesellschaft mbH, formerly known as eleven Gesellschaft zur Entwicklung und Vermarktung von Netzwerktechnologien mbH.

A. Selected financial data

The selected consolidated statements of income data for the years ended December 31, 2011, 2012 and 2013 and the selected consolidated balance sheet data as of December 31, 2012 and 2013 have been derived from the Consolidated Financial Statements of CYREN included elsewhere in this Annual Report on Form 20-F, or this Annual Report. The selected consolidated statements of operations data for the years ended December 31, 2009 and 2010 and the selected consolidated balance sheet data as of December 31, 2009, 2010 and 2011 have been derived from the Consolidated Financial Statements of CYREN not included elsewhere in this Annual 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,				
	2009	2010	2011	2012	2013
	(USD and share amounts in thousands, except per share data)				
Selected Data:					
Revenues	$15,189	$18,161	$23,016	$23,910	$32,248
Operating income (loss)	$2,696	$3,360	$3,308	$780	$(2,107)
Net income (loss) attributable to ordinary and equivalently participating shareholders	$5,160	$4,403	$4,598	$1,485	$(9,871)
Operating income (loss) per share	$0.11	$0.14	$0.14	$0.03	$ (0.08)
Basic net earnings (loss) per share	$0.21	$0.19	$0.19	$0.06	$(0.38)
Diluted operating income (loss) per share	$0.11	$0.14	$0.13	$0.03	$(0.08)
Diluted net earnings (loss) per share	$0.20	$0.18	$0.19	$0.06	$(0.38)
Weighted average number of shares used in computing basic net earnings per share	24,532	23,575	23,620	24,610	26,231
Weighted average number of shares used in computing diluted net earnings per share	25,292	24,874	24,654	25,140	26,231
Total Assets	$25,190	$31,982	$39,534	$59,133	$50,933

B. Capitalization and indebtedness

Not applicable

C. Reason for the offer and use of proceeds

Not applicable

D. Risk factors

1

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 similar 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 our actual results, performance, levels of activity, or achievements, or industry results, to be materially different from those 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

Our business faces significant risks. You should carefully consider all of the information set forth in this annual report and in our other filings with the SEC, including the following risk factors which we face and which are faced by our industry. Our business, financial condition and results of operations could be materially adversely affected by any of these risks. This report also contains forward-looking statements that involve risks and uncertainties. Our results could materially differ from those anticipated in these forward-looking statements, as a result of certain factors including the risks described below and elsewhere in this report and our other SEC filings. See also "Forward-Looking Statements".

Business Risks

If the Internet security market does not accept our new cloud-based product offerings, our sales will not grow as quickly as anticipated, or at all, and our business, results of operations and financial condition would be harmed.

We are seeking to exploit our new cloud-based security platform, CYREN Web Security (CWS) to disrupt the Internet security market and our historic business model. Our success will depend to a substantial extent on the willingness of enterprises, large and small, to increase their use of cloud computing services. The market for messaging security and compliance solutions delivered as a service in particular is at an early stage relative to on-premise solutions, and these applications may not achieve and sustain high levels of demand and market acceptance.

Historically, companies have used signature-based security products, such as firewalls, intrusion prevention systems, or IPS, anti-virus, or AV, and web and messaging gateways, for their IT security. These enterprises may be hesitant to purchase our cloud-based security offering if they believe that our signature-based products or those of our competitors are more cost-effective, provide substantially the same functionality or otherwise provide a sufficient level of IT security. Many enterprises have invested substantial personnel and financial resources to integrate traditional enterprise software or hardware appliances for these applications into their businesses, and currently, most enterprises have not allocated a fixed portion of their budgets to protect against next-generation advanced cyber attacks. As a result, to expand our customer base, we need to convince potential customers to allocate a portion of

their discretionary budgets to purchase our products and services. If we do not succeed in convincing customers that our offerings should be an integral part of their overall approach to IT security, our sales will not grow as quickly as anticipated, or at all, which would have an adverse impact on our business, results of operations and financial condition.

In addition, many enterprises may be reluctant or unwilling to use cloud computing services because they have concerns regarding the risks associated with its reliability and security, among other things, of this delivery model, or its ability to help them comply with applicable laws and regulations. If enterprises do not perceive the benefits of this delivery model, then the market for our services and our sales would not grow as quickly as we anticipate or at all and our business, results of operations and financial condition would be harmed.

If the market does not continue to respond favorably to our traditional Internet security solutions, including our CYREN EmailSecurity, antispam solutions, embedded antivirus, new cloud-based solutions or Uniform Resource Locator (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 traditional Internet security solutions by current and new businesses, Original Equipment Manufacturers, or OEMs, and service provider customers, plus the interest of such customers in our newest offerings. We have been selling our inbound anti-spam products for over nine years, our Zero-Hour™ virus outbreak detection product for approximately eight years, our GlobalView™ Mail Reputation perimeter defense solution for approximately seven years, our URL filtering solutions for over five years, our outbound spam solution for approximately three years and the CYREN Antivirus solution for over four years.

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 top end solutions to keep their performance at an industry-acceptable 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, results of operations and financial condition will suffer dramatically.

If we are unable to effectively integrate recent and future acquisitions and investments, our business operations and financial results will suffer.

Our success will depend, in part, on our ability to expand our service and product offerings and grow our business in response to changing technologies, customer demands and competitive pressures. In some circumstances, we may decide to do so through the acquisition of complementary businesses and technologies rather than through internal development, including, for example, our 2012 acquisition of the antivirus business of the Icelandic company, Frisk Software International (“Frisk”) and the German Internet security company eleven GmbH (“eleven”). For a relatively small organization such as CYREN, the acquisition of two companies within less than six months, in two very different parts of the world, is an extremely complex and challenging venture.

If we encounter further difficulties or unforeseen expenditures in integrating the business, technologies, products, personnel or operations of these companies or any other company that we acquire, the revenue and operating results of the combined company could be adversely affected. The risks we face in connection with acquisitions, including those we are facing in our recent acquisitions of Frisk and eleven, include:

- disruption of our ongoing business, diversion of resources, increased expenses and distraction of our management from operating our business to addressing acquisition integration challenges;
- additional legal and regulatory compliance ;
- cultural challenges associated with integrating employees from the acquired companies into our organization;
- inability to retain key employees from the acquired companies;
- inability to strengthen our competitive position, achieve our strategic goals, generate sufficient financial return to offset acquisition costs or realize the expected benefits of the acquisition;
- failure to identify significant problems or liabilities, including liabilities resulting from the acquired companies' pre-acquisition failure to comply with applicable laws, during our pre-acquisition due diligence;

- entry into geographic or business markets in which we have little or no prior experience or where competitors have stronger market positions;
- difficulties in, or inability to, successfully sell any acquired products or services;
- coordination of research and development, sales and marketing, accounting, human resources and other general and administrative systems;
- changes in relationships with strategic partners as a result of product acquisitions or strategic positioning resulting from the acquisitions;
- liability for activities of the acquired companies before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities and litigation; and
- unanticipated write-offs or charges.

The occurrence of any of these risks could have a material adverse effect on our business operations and financial results.

We face intense competition and could lose market share to our competitors, which could adversely affect our business, financial condition and results of operations.

The market for security products and services is intensely competitive and characterized by rapid changes in technology, customer requirements, industry standards and frequent new product introductions and improvements. We anticipate continued challenges from current competitors, which in many cases enjoy greater resources than us, as well as by new entrants into the industry. If we are unable to anticipate or effectively react to these competitive challenges, our competitive position could weaken, and we could experience a decline in our revenue that could adversely affect our business and results of operations.

Many of our existing competitors have, and some of our potential competitors could have, substantial competitive advantages such as:

- greater name recognition and larger customer bases;
- larger sales and marketing budgets and resources;
- broader distribution and established relationships with channel and distribution partners and customers;
- greater customer support resources;
- direct selling to end users;
- lower labor and research and development costs; and
- substantially greater financial, technical and other resources.

In addition, some of our larger competitors have substantially broader product offerings and may be able to leverage their relationships with distribution partners and customers based on other products or incorporate functionality into existing products to gain business in a manner that discourages users from purchasing our products, subscriptions and services, including by selling at zero or negative margins, product bundling or offering closed technology platforms. Some of our competitors also sell directly to end users and, therefore, have a larger addressable market.

Potential customers may also prefer to purchase from their existing suppliers rather than a new supplier regardless of product performance or features. As a result, even if the features of our offerings are superior, customers may not purchase our services or products. In addition, innovative start-up companies, and larger companies that are making significant investments in research and development, may invent similar or superior products and technologies that compete with our product and services. Our current and potential competitors may also establish cooperative relationships among themselves or with third parties that may further enhance their resources. If we are unable to compete successfully, or if competing successfully requires us to take costly actions in response to the actions of our competitors, our business, financial condition and results of operations could be adversely affected.

Some of our competitors have acquired businesses that may allow them to offer more directly competitive and comprehensive solutions than they had previously offered, such as Proofpoint's acquisition of Sendmail and Armorize, IBM's acquisition of Trusteer, Blue Coat's acquisition of Solera, FireEye's acquisition of Mandiant, and Palo Alto's acquisition of Cyvera. As a result of such acquisitions, our current or potential competitors might be able to adapt more quickly to new technologies and end user needs, devote greater resources to the promotion or sale of their products and services, initiate or withstand substantial price competition, take advantage of acquisitions or other opportunities more readily, or develop and expand their product and service offerings more quickly than we can. Due to various reasons, organizations may be more willing to incrementally add solutions to their existing security infrastructure from competitors than to replace it with our solutions. These competitive pressures in our market or our failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margins, and

loss of market share. Any failure to meet and address these factors could seriously harm our business and operating results.

Also, many of our smaller competitors that specialize in providing protection from a single type of business security threat may deliver these specialized business security products to the market more quickly than we can or may introduce innovative new products or enhancements before we do. Conditions in our markets could change rapidly and significantly as a result of technological advancements.

If we are unable to enhance our existing solutions and develop new solutions, our growth will be harmed.

Our ability to attract new customers and increase revenue from existing customers will depend in large part on our ability to enhance and improve our existing solutions and to introduce new solutions. The success of any enhancement or new solution depends on several factors, including the timely completion, introduction and market acceptance of the enhancement or solution. Any enhancement or solution we develop or acquire may not be introduced in a timely or cost-effective manner and may not achieve the broad market acceptance necessary to generate significant revenue. If we are unable to successfully develop or acquire new solutions or enhance our existing solutions to meet customer requirements, we may not grow as expected.

We cannot be certain that our development activities will be successful or that we will not incur delays or cost overruns. Furthermore, we may not have sufficient financial resources to identify and develop new technologies and bring enhancements or new solutions to market in a timely and cost-effective manner. New technologies and enhancements could be delayed or cost more than we expect, and we cannot ensure that any of these solutions will be commercially successful if and when they are introduced.

Adverse conditions in the national and global financial markets could have a material adverse effect on our business, operating results and financial condition.

Our financial performance depends, in part, on the state of the economy, which deteriorated in the recent broad recession, and which may further deteriorate in the future. Challenging economic conditions worldwide have from time to time contributed, and may continue to contribute, to slowdowns in the information technology industry, resulting in reduced demand for our solutions as a result of continued constraints on IT-related capital spending by our customers and increased price competition for our solutions.

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 and service provider 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 the perceived general level of advanced cyber attacks declines, demand for our solutions may decrease, our cost of doing business may increase and our business could be harmed.

Our business is substantially dependent on enterprises recognizing that advanced cyber attacks are pervasive and are not effectively prevented by legacy security solutions. High visibility attacks on prominent enterprises and governments have increased market awareness of the problem of advanced cyber attacks and help to provide an impetus for enterprises to devote resources to protecting against advanced cyber attacks, such as purchasing our services and products and broadly deploying our services and products within their organizations. If advanced cyber attacks were to decline, or enterprises perceived that the general level of advanced cyber attacks have declined, our ability to attract new customers and expand our offerings within existing customers could be materially and adversely affected. A reduction in the threat landscape could increase our sales cycles and harm our business, results of operations and financial condition.

In addition, various state legislatures have enacted laws aimed at regulating the distribution of unsolicited email. 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 resellers to sell all of our products, and if our partners fail to perform, our ability to sell and distribute our products and services will be limited, and our operating results will be harmed.

We expect to continue to be dependent upon OEM partners and service providers for a significant portion of our revenues, which will be derived from sales of our messaging, antivirus and web security solutions. We also expect resellers to become important in the distribution of our newer cloud-based Internet security solutions such as CYREN WebSecurity (“CWS”).

We anticipate that in the future we will derive a substantial portion of the sales of CWS through channel partners. In order to scale our channel program to support growth in our business, it is important that we help our partners enhance their ability to independently sell and deploy our solutions. We may be unable to successfully expand and improve the effectiveness of our channel sales program.

Our operating results and financial condition may be materially adversely affected if:

- anticipated orders or payments from these customers fail to materialize;
- our customers cease the promotion of our business or begin to promote additional solutions;

- our customers are acquired by larger companies who may have other relationships or technologies that lead to the displacement or termination of CYREN contracts;
- our customers do not live up to their contractual agreements or fail to pay for services rendered; or
- our customers' businesses fail.

If we are unable to maintain our relationships with these channel partners, or otherwise develop and expand our indirect distribution channel, our business, results of operations, financial condition or cash flows could be adversely affected.

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

Our revenues and operating results could vary significantly from period to period as a result of a variety of factors, many of which are outside of our control. As a result, comparing our revenues and operating results on a period-to-period basis may not be meaningful, and you should not rely on our past results as an indication of our future performance. We may not be able to accurately predict our future revenues or results of operations. We base our current and future expense levels on our operating plans and sales forecasts, and our operating costs are relatively fixed in the short-term. As a result, we may not be able to reduce our costs sufficiently to compensate for an unexpected shortfall in revenues, and even a small shortfall in revenues could disproportionately and adversely affect financial results for that quarter. In addition, we recognize revenues from sales to some customers or resellers when cash is received, which may be delayed because of issues with those customers or resellers. If our revenues or operating results fall below the expectations of investors or any securities analysts that cover our stock, the price of our common stock could decline substantially.

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 both our traditional messaging, antivirus and web security solutions and our newer cloud-based Internet 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 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 CYREN.

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. We continue to be substantially dependent on our sales force to obtain new customers and to drive additional use cases and adoption among our existing customers. We believe that there is significant competition for sales personnel with the skills and technical knowledge that we require. Our ability to achieve significant revenue growth will depend, in large part, on our success in recruiting, training and retaining sufficient numbers of sales personnel to support our growth. New hires require significant training and may take significant time before they achieve full productivity. Our recent hires and planned hires may not become productive as quickly as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business.

Our future success depends on our ability to sell additional solutions to our customers. This may require increasingly sophisticated and costly sales efforts and may not result in additional sales. In addition, the rate at which our customers purchase additional solutions depends on a number of factors, including the perceived need for additional solutions, growth in the number of end users, and general economic conditions. If our efforts to sell additional solutions to our customers are not successful, our business, financial condition and/or results of operations may suffer.

We rely on our management team and other key employees and will need additional personnel to grow our business, and the loss of one or more key employees or our inability to attract and retain qualified personnel could harm our business.

Our success is substantially dependent on our ability to attract, retain and motivate the members of our management team and other key employees throughout our organization. Competition for highly skilled personnel is intense, especially in Israel, Berlin, Reykjavík, Palo Alto, and the Washington D.C. area, where we have an office and a need for highly skilled personnel. We may not be successful in attracting qualified personnel to fulfill our current or future needs. Our competitors may be successful in recruiting and hiring members of our management team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. Also, to the extent we hire employees from mature public companies with significant financial resources, we may be subject to allegations that such employees have been improperly solicited, that they have divulged proprietary or other confidential information or that their former employers own such employees' inventions or other work product.

In addition, we believe that it is important to establish and maintain a corporate culture that facilitates the maintenance and transfer of institutional knowledge within our organization and also fosters innovation, teamwork, a passion for customers and a focus on execution. Our Chief Executive Officer and certain other key members of our management and finance teams have only been working together for a relatively short period of time. If we are not successful in integrating these key employees into our organization, such failure could delay or hinder our product development efforts and the achievement of our strategic objectives, which could adversely affect our business, financial condition and results of operations.

The loss of our software developers or senior operations personnel may also adversely affect the continued development and support of both our current messaging, antivirus and web security solutions and future solutions presently included in our roadmap for development, 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. If one or more of our key employees resigns or otherwise ceases to provide us with their service, our business, financial condition and/or results of operations could be harmed.

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

We market and sell our products throughout the world and have personnel in many parts of the world. In addition, we have sales offices and research and development facilities outside the United States and we conduct, and expect to continue to conduct, a significant amount of our business with companies that are located outside the United States, particularly in Israel, Asia and Europe. We also enter into strategic distributor and reseller relationships with companies in certain international markets where we do not have a local presence. If we are not able to maintain successful strategic distributor relationships internationally or recruit additional companies to enter into strategic distributor relationships, our future success in these international markets could be limited. Business practices in the international markets that we serve may differ from those in the United States and Israel and may require us in the

future to include terms other than our standard terms in customer contracts, although to date we generally have not done so. To the extent that we enter into customer contracts in the future that include non-standard terms related to payment, warranties, or performance obligations, our operating results may be adversely impacted.

Additionally, our international sales and operations are subject to a number of risks, including the following:

- greater difficulty in enforcing contracts and accounts receivable collection and longer collection periods;
- the uncertainty of protection for intellectual property rights in some countries;
- greater risk of unexpected changes in regulatory practices, tariffs, and tax laws and treaties;
- risks associated with trade restrictions and foreign legal requirements, including the importation, certification, and localization of our products required in foreign countries;
- the potential that our operations in Israel and the U.S. may limit the acceptability of our products to some foreign governments, and vice versa;

- greater risk of a failure of foreign employees, partners, distributors, and resellers to comply with both U.S. and foreign laws, including antitrust regulations, and any trade regulations ensuring fair trade practices;

- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements;

- the potential for acts of terrorism, hostilities or war;

- increased expenses incurred in establishing and maintaining office space and equipment for our multinational operations;

- greater difficulty in recruiting local experienced personnel, and the costs and expenses associated with such activities;

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

- fluctuations in exchange rates between the U.S. dollar, NIS and foreign currencies in markets where we do business; and

- general economic and political conditions and uncertainties in these foreign markets.

These factors and other factors could harm our ability to gain future international revenues and, consequently, materially impact our business, operating results, and financial condition. The expansion of our existing international operations and entry into additional international markets will require significant management attention and financial resources.

Our web security solutions may be adversely affected if we are not able to receive sufficient components from third party suppliers.

Our web security solution relies in part on certain components supplied by third parties 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 solution may not perform at the level we expect. If this were to occur, the effectiveness of this solution would drop, it 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, antimalware and web security industries are characterized by difficult technological challenges, sophisticated distributors of Internet security threats, multiple-variant viruses, advance persistent threats, 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, antimalware 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.

Many of our end users operate in markets characterized by rapidly changing technologies and business plans, which require them to adapt to increasingly complex IT networks, incorporating a variety of hardware, software applications,

operating systems and networking protocols. As their technologies and business plans grow more complex, we expect these customers to face new and increasingly sophisticated methods of attack. We face significant challenges in ensuring that our solutions effectively identify and respond to these advanced and evolving attacks without disrupting our customers' network performance. As a result of the continued rapid innovations in the technology industry, including the rapid growth of smart phones, tablets and other devices and the trend of "bring your own device" in enterprises, we expect the networks of our end users to continue to change rapidly and become more complex.

We have identified a number of new products and enhancements to our platform that we believe are important to our continued success in the IT security market. For example, in February 2014, we announced the introduction of CWS, our first service launched through our cloud infrastructure that offers end users secure browsing from any device, anywhere. We may not be successful in developing and marketing, on a timely basis, such new products or enhancements or that our new products or enhancements will adequately address the changing needs of the marketplace. In addition, some of our new products and enhancements may require us to develop new architectures that involve complex, expensive and time-consuming research and development processes. Although the market expects rapid introduction of new products and enhancements to respond to new threats, the development of these products and enhancements is difficult and the timetable for commercial release and availability is uncertain, as there can be significant time lags between initial beta releases and the commercial availability of new products and enhancements. We may experience unanticipated delays in the availability of new products and enhancements to our platform and fail to meet customer expectations with respect to the timing of such availability. If we do not quickly respond to the rapidly changing and rigorous needs of our customers by developing, releasing and making available on a timely basis new products and enhancements to our services and products that can adequately respond to advanced threats and our customers' needs, our competitive position and business prospects will be harmed. Furthermore, from time to time, we or our competitors may announce new products with capabilities or technologies that could have the potential to replace or shorten the life cycles of our existing services products. Announcements of new products could cause customers to defer purchasing our existing services or products.

Additionally, the process of developing new technology is expensive, complex and uncertain. The success of new products and enhancements depends on several factors, including appropriate component costs, timely completion and introduction, differentiation of new products and services from those of our competitors, and market acceptance. To maintain our competitive position, we must continue to commit significant resources to developing new products or services before knowing whether these investments will be cost-effective or achieve the intended results. We may not be able to successfully identify new product opportunities, develop and bring new products or services to market in a timely manner, or achieve market acceptance of our platform. Products and technologies developed by others may render our offerings obsolete or noncompetitive. If we expend significant resources on researching and developing products or services and such products and services are not successful, our business, financial position and results of operations may be adversely affected. We may not be able to use new technologies effectively or adapt to OEM, service provider, customer or end user requirements or emerging industry standards.

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

Our messaging, antimalware 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 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, antimalware 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, financial condition and/or results of operations to suffer.

Real or perceived defects, errors or vulnerabilities in our services or the failure of our services to block malware or prevent a security breach could harm our reputation and adversely impact our business, financial condition and results of operations.

Because our products and services are complex, they have contained and may contain design or manufacturing defects or errors that are not detected until after their commercial release and deployment by our end users. For example, from time to time, certain of our end users have reported defects in our products related to performance, scalability and compatibility that were not detected before offering the service. Additionally, defects may cause our products or services to be vulnerable to security attacks, cause them to fail to help secure networks or temporarily interrupt end users' networking traffic. Because the techniques used by computer hackers to access or sabotage networks change frequently and generally are not recognized until launched against a target, we may be unable to anticipate these techniques and provide a solution in time to protect our end users' networks. Furthermore, as a well-known provider of Internet security solutions, our networks, products, and services could be targeted by attacks specifically designed to disrupt our business and harm our reputation. Our data centers and networks may experience technical failures and downtime, may fail to distribute appropriate updates, or may fail to meet the increased requirements of a growing end user base, any of which could temporarily or permanently expose our end users' networks, leaving their networks unprotected against the latest security threats.

Any real or perceived defects, errors or vulnerabilities in our services, or any other failure of our services to detect an advanced threat, could result in:

- a loss of existing or potential customers or channel partners;

- delayed or lost revenue;
- a delay in attaining, or the failure to attain, market acceptance;
- the expenditure of significant financial and product development resources in efforts to analyze, correct, eliminate, or work around errors or defects, to address and eliminate vulnerabilities, or to identify and ramp up production with alternative third-party manufacturers;
- an increase in warranty claims, or an increase in the cost of servicing warranty claims, either of which would adversely affect our gross margins;

- harm to our reputation or brand; and
- litigation, regulatory inquiries or investigations that may be costly to address and further harm our reputation.

Data thieves are sophisticated, often affiliated with organized crime and operate large scale and complex automated attacks. In addition, their techniques change frequently and generally are not recognized until launched against a target. If we fail to identify and respond to new and complex methods of attack and to update our services to detect or prevent such threats in time to protect our end users' systems, our business and reputation will suffer.

An actual or perceived security breach or theft of the sensitive data of one of our end users, regardless of whether the breach is attributable to the failure of our products or services, could adversely affect the market's perception of our security offerings. Despite our best efforts, there is no guarantee that our products and services will be free of flaws or vulnerabilities, and even if we discover these weaknesses we may not be able to correct them promptly, if at all. Our end user customers may also misuse our products and services, which could result in a breach or theft of business data.

Our messaging, antimalware 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, antimalware 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.

False detection of applications, viruses, malware, spyware, vulnerability exploits, data patterns or URL categories could adversely affect our business.

Our classifications of application type, virus, malware, spyware, vulnerability exploits, data, or URL categories may falsely detect applications, content or threats that do not actually exist. This risk is heightened by the inclusion of a "heuristics" feature in our products, which attempts to identify applications and other threats not based on any known signatures but based on characteristics or anomalies which indicate that a particular item may be a threat. These "false positives", while typical in our industry, may impair the perceived reliability of our products and may therefore adversely impact market acceptance of our services and products. If our services and products restrict important files or applications based on falsely identifying them as malware or some other item that should be restricted, this could adversely affect end users' systems and cause material system failures. Any such false identification of important files or applications could result in damage to our reputation, negative publicity, loss of end users and sales, increased costs to remedy any problem, and costly litigation.

Our new cloud-based SecaaS offerings are nascent service offerings, so we may not see the customer traction in these offerings that we anticipate.

Security as a Service (SecaaS) is a model of cloud-based services offerings. In February 2014, we released CWS, our cloud-based security service that provides end users secure browsing from any device, anywhere. CWS is our push into the cloud-based Internet security sector. The solutions we are promoting and will promote to this market will enable Internet security vendors and service providers to offer fully cloud-based, Internet security solutions to their customers, without the need for the integration of a software development kit, or SDK, into their product offerings. Among other things, this cloud-based approach is intended to speed up the process of moving our solutions

to market, and ease the integration burden for our customers.

In recent years, companies have begun to expect that key security software services, such as URL filtering, be provided through a SecaaS model. In order to provide CWS via a SecaaS deployment, we have made and will continue to make capital investments to implement this alternative business model, which could negatively affect our financial results. Even with these investments, the SecaaS business model for CWS may not be successful. Because of the newness of the technologies involved and the resulting learning curve required of all employees in the sale and support of the new offerings, we cannot be certain that we will convince potential customers of the benefits of these new offerings and sell them at the rate we anticipate. If we fall short of our expectations, and especially given the significant resources invested by us in bringing these new offerings to market, our financial results will suffer and the value of shareholder investments will decline.

If we fail to develop or protect our new brand CYREN, our business may be harmed.

In January 2014, we announced the Company would change its name from Commtouch to CYREN. We adopted our new name as we completed our transformation into a leading provider of cloud-based information security solutions that are specially designed to be deployed or private labeled by customers and partners alike. Developing and maintaining awareness and integrity of our company and our new brand are important to achieving widespread acceptance of our existing and future offerings and are important elements in attracting new customers. The importance of brand recognition will increase as competition in our market further intensifies. Successful promotion of our brand will depend on the effectiveness of our marketing efforts and on our ability to provide reliable and useful solutions at competitive prices. We plan to continue investing substantial resources to promote our brand, both domestically and internationally, but there is no guarantee that our brand development strategies will enhance the recognition of our brand. Some of our existing and potential competitors have well-established brands with greater recognition than we have. If our efforts to promote and maintain our brand are not successful, our operating results and our ability to attract and retain customers may be adversely affected. In addition, even if our brand recognition and loyalty increases, this may not result in increased use of our solutions or higher revenue.

Investment Risks

Our failure to raise additional capital or generate the significant capital necessary to expand our operations and invest in new services and products could reduce our ability to compete and could harm our business.

We intend to continue to make investments to support our business growth and may require additional funds to respond to business challenges, including the need to develop new features to enhance our services and products, improve our operating infrastructure or acquire complementary businesses and technologies. Accordingly, we may need to engage in equity or debt financings to secure additional funds. If we raise additional equity financing, our stockholders may experience significant dilution of their ownership interests and the per share value of our common stock could decline. Furthermore, if we engage in debt financing, the holders of debt would have priority over the holders of common stock, and we may be required to accept terms that restrict our ability to incur additional indebtedness or that otherwise restrict our ability to operate our business. We may also be required to take other actions that would otherwise be in the interests of the debt holders and force us to maintain specified liquidity or other ratios, any of which could harm our business, operating results, and financial condition. We may not be able to obtain additional financing on terms favorable to us, if at all. If we are unable to obtain adequate financing or financing on terms satisfactory to us when we require it, our ability to continue to support our business growth and to respond to business challenges could be significantly impaired, and our business may be adversely affected.

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.

Our CEO, Lior Samuelson, is also Chairman of our Board of Directors. 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 22.8% of our outstanding Ordinary Shares as of April 1, 2014. 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 April 1, 2014). 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 many 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 CYREN. 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 often trade at different prices on NASDAQ and TASE.

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.

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.

Risks Relating to Operations in Israel

Conditions in Israel may limit our ability to develop and sell our products, resulting in a decline in revenues.

We are incorporated under the laws of the State of Israel. Our principal research and development facilities are located in Israel. Since the establishment of the State of Israel in 1948, a number of armed conflicts have taken place between Israel and its neighboring countries, as well as incidents of civil unrest, and a number of state and non-state actors have publicly committed to its destruction. Political, economic and military conditions in Israel could directly affect our operations. We could be adversely affected by any major hostilities involving Israel, including acts of terrorism or any other hostilities involving or threatening Israel, the interruption or curtailment of trade between Israel and its trading partners, a significant increase in inflation or a significant downturn in the economic or financial condition of Israel. Any on-going or future violence between Israel and the Palestinians, armed conflicts, terrorist activities, tension along the Israeli borders or with other countries in the region, including Iran, or political instability in the region could disrupt international trading activities in Israel and may materially and negatively affect our business and could harm our results of operations.

Certain countries, as well as certain companies and organizations, continue to participate in a boycott of Israeli firms, firms with large Israeli operations and others doing business with Israel and Israeli companies. In addition, such boycott, restrictive laws, policies or practices may change over time in unpredictable ways, and could, individually or in the aggregate, have a material adverse effect on our business in the future.

Some of our employees in Israel, including some of our executive officers, are obligated to perform annual military reserve duty in the Israel Defense Forces, depending on their age and position in the armed forces. Furthermore, they may be called to active reserve duty at any time under emergency circumstances for extended periods of time. For example, in 2013, approximately four of our employees in Israel were called for active reserve duty, each serving for an average of approximately two weeks. Our operations could be disrupted by the absence, for a significant period, of one or more of our executive officers or key employees due to military service, and any significant disruption in our operations could 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 Euros, 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 2013, 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.

Through a program with the Office of the Chief Scientist of the Israeli Ministry of Industry, Trade & Labor, or OCS, we received grants from the Government of Israel, to finance a significant portion of our research and development expenditures in Israel. In 2012 and 2013, we received $169 thousand and $416 thousand, respectively.

In order to meet specified conditions in connection with grants and programs of the OCS, we have made representations to the Israel government about our Israeli operations. The grant requires a minimum commitment of three years and we are required to share information with other companies and academics. 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.

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.

CYREN Ltd. is organized under the laws of Israel, and we maintain significant operations in Israel. In addition, most of our assets are located outside the United States. Service of process upon our non-U.S. resident directors and enforcement of judgments obtained in the United States against them and CYREN Ltd. may be difficult to obtain within the United States. It may be difficult to enforce civil causes of actions under U.S. securities law 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 CYREN Ltd., 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 officers, directors or significant shareholders and regulates other matters that may be relevant to these types of transactions. Furthermore, Israeli tax considerations may make potential transactions unappealing to us or to our shareholders whose country of residence does not have a tax treaty with Israel exempting such shareholders from Israeli tax. For example, Israeli tax law does not recognize tax-free share exchanges to the same extent as U.S. tax law. With respect to mergers, Israeli tax law allows for tax deferral in certain circumstances but makes the deferral contingent on the fulfillment of a number of conditions, including a holding period of two years from the date of the transaction during which sales and dispositions of shares of the participating companies are subject to certain restrictions. Moreover, with respect to certain share swap transactions, the tax deferral is limited in time, and when such time expires, the tax becomes payable even if no disposition of the shares has occurred.

These and other similar provisions could delay, prevent or impede an acquisition of our company or our merger with another company, even if such an acquisition or merger would be beneficial to us or to our shareholders

Your rights and responsibilities as a shareholder will be governed by Israeli law which differs in some respects from the rights and responsibilities of shareholders of U.S. companies.

We are incorporated under Israeli law. The rights and responsibilities of the holders of our ordinary shares are governed by our Articles of Association and Israeli law. These rights and responsibilities differ in some respects from the rights and responsibilities of shareholders in typical U.S.-based corporations. In particular, a shareholder of an Israeli company has a duty to act in good faith toward the company and other shareholders and to refrain from abusing its power in the company, including, among other things, in voting at the general meeting of shareholders on matters such as amendments to a company's articles of association, increases in a company's authorized share capital, mergers and acquisitions and interested party transactions requiring shareholder approval. In addition, a shareholder who knows that it possesses the power to determine the outcome of a shareholder vote or to appoint or prevent the appointment of a director or executive officer in the company has a duty of fairness toward the company. There is limited case law available to assist us in understanding the implications of these provisions that govern shareholders' actions. These provisions may be interpreted to impose additional obligations and liabilities on holders of our ordinary shares that are not typically imposed on shareholders of U.S. corporations.

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 our Board of Directors, or Board, and quorum requirements 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.

A. History and development of the Company

We were incorporated as a private company under the laws of the State of Israel on February 10, 1991 and our legal form is a company limited by shares. We became a public company on July 15, 1999 under the name Commtouch Software Ltd. In January 2014, we changed our legal name to CYREN Ltd.

Our principal executive offices are located at 1 Sapir Rd., 5th Floor, Beit Ampa, P.O. Box 4014, Herzliya, 46140 Israel, where our telephone number is 972–9–863–6888. Our Amended and Restated Articles of Association, or 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.

Our authorized agent in the United States is our subsidiary, CYREN Inc. located at 7925 Jones Branch Drive, Suite 5200, McLean, Virginia 22102.

PROPERTY AND EQUIPMENT, NET

	Year Ended December 31,		
	2011	2012	2013
	(in thousands)		
Cost:			
Computers and peripheral equipment	$4,717	$5,848	$7,350
Office furniture and equipment	640	848	1,112
Motor vehicles	45	10	10
Leasehold improvements	1,195	1,225	1,581
	6,597	7,931	10,053
Less accumulated depreciation	(5,712)	(6,323)	(7,379)
Property and equipment, net	$885	$1,608	$2,674

The Company finances the capital expenditures from operations. The Company continues to invest in capital expenditures that support the growth of the Company's business and support the rollout of new products and services.

B. Business Overview

CYREN is a global leader in information security solutions for protecting web, email and mobile transactions. We are a pioneering security-as-a-service provider of integrated cloud-based security technology providing cost-effective, easily deployed solutions that mitigate external and internal threats, including modern cyber-threats, advanced malware attacks, information leaks, legal liability and productivity loss through global data detection, prevention and intelligence. CYREN delivers innovative security services and detection technologies, designed to protect end users from virus, phishing and malware attacks across all their devices, wherever end users are.

Organizations rely on the Internet and email to conduct business, and frequently send critical or confidential information outside their network perimeters as part of their established business processes. Accelerating use of rich web-based applications with real-time interaction, social web sites with user-generated content, and the rise of cloud services, are increasing the volume and value of information transmitted across the Internet. At the same time, the cost and number of security breaches involving data loss has increased, and regulatory compliance requirements have become more stringent. These trends support the need for unified, organization-wide web and email security solutions that include data loss prevention capabilities and address the dynamic nature of both web content and cyber-threats.

A fundamental shift in the sources of cyber crime, from hackers to organized crime and governments, combined with the emergence of international data trafficking and sophisticated advanced persistent threats ("APTs"), polymorphic threats, zero-day exploits, and user-transplant "drive-by" downloads, is driving an unprecedented wave of targeted, malicious attacks designed to steal valuable information. At the same time, the growth of business-to-business collaboration, as well as the consumerization of IT and the associated adoption of mobile devices and unmanaged Internet-based applications, has proliferated sensitive data and reduced the effectiveness of many existing security products. These factors have contributed to an increasing number of severe data breaches and expanding regulatory mandates, all of which have accelerated demand for effective data protection and security solutions.

CYREN is a leading provider of cloud-based security solutions that deliver powerful protection through global data intelligence. Regardless of the device or its location, CYREN's easily deployed web, email, and antimalware products deliver uncompromising protection in both embedded and security-as-a-service deployments. Organizations rely on

CYREN's cloud-based threat detection and proactive security analytics to provide up-to-date spam classifications, URL categorization and malware detection services. The CYREN GlobalView™ cloud security platform leverages Recurrent Pattern Detection™ technologies to protect more than 550 million users in 190 countries.

As a trusted technology partner, CYREN provides our services to a wide array of customers and OEM and service provider distribution partners, including network and security vendors offering content security gateways, unified threat management, or "UTM", solutions, network appliances, antivirus solutions and to service providers such as Software-as-a-Service, or SaaS, vendors, web hosting providers and Internet service providers. With extensive OEM experience, dedicated Technical Account Management (TAM), and a customer success program, CYREN partners with our customers to help ensure success at both the technical and sales levels. Our customers include leading vendors and service providers such as:

- web hosters and ISPs
- SaaS/SecaaS providers
- Networking hardware manufacturers
- Security devices and software manufacturers
- Content security gateways

We have invented a purpose-built, cloud-based security service that provides real-time protection to enterprises worldwide that are facing the next generation of cyber attacks. Our technology approach represents a paradigm shift in how IT security has been conducted since the earliest days of the information technology industry.

The core of our purpose-built, cloud-based security platform is CYREN's GlobalViewTM and patented Recurrent Pattern Detection™ (RPD™) technologies which identify and protect against known and unknown threats that existing signature-based technologies are unable to detect.

The GlobalView cloud infrastructure has been operational for over 15 years and is built from multiple high-availability data centers worldwide. In addition, global points of presence ensure low latency as well as local data handling where required by country-specific legislation. End users may be routed to the CYREN cloud using a variety of options. All organizational traffic may be directed using proxy-chaining, port forwarding, or GRE tunneling. Alternatively, for roaming users, PAC (Proxy Auto Config) files may be used. CYREN also supports smartphones and tablets with a range of solutions for Android and iOS operating systems with mobile users routed through the most secure VPN tunnel.

Our Offerings

Our Offerings

The CYREN portfolio of services are grouped into solution suites:

Web – protection on any device, anywhere
Email – guards email inboxes from outbound and incoming attacks
AntiMalware – proactive security to combat new and emerging threats

Our services are deployed through various means, including (i) through the integration of an SDK, which, upon integration, is then able to communicate with our worldwide cloud detection centers that provide our customers and users with the most up to date protection against the latest Internet threats; and (ii) through our cloud-based Secaas platform.

CYREN WebSecurity (CWS)

The fast-growing web Security as a Service (SecaaS) market provides a tremendous opportunity to vendors and service providers who are able to enter

this space. There are several reasons for the fast adoption of the SecaaS cloud model including: an increasingly mobile workforce; the bring your own device (BYOD) trend; business and user applications that have moved to the cloud; the increased cost and complexity of managing a myriad of on-site solutions across multiple remote offices. These factors have created a shift in the way small and medium businesses and enterprises are looking to consume web security. There are also the additional needs of compliance – ensuring that inappropriate or illegal sites are not visited from company infrastructure - and employee productivity – ensuring that company time and bandwidth is not wasted on unnecessary web usage.

CYREN has developed our proprietary solution, CYREN WebSecurity (CWS), for cloud-based protection of our customer's devices against web-borne threats. CWS includes cloud based URL filtering and antimalware protection. CWS has been designed and built from the ground up as a private-label service to enable our partners to quickly enter this exciting market. CWS can be deployed through multiple channels, versatile multi-tenant partner, reseller, distributor, and customer relationships enable any channel, licensing, or sales ecosystem. CWS has an intuitive web interface that streamlines provisioning and configuration tasks for all partner tiers and for all organizational resources including mobile. CWS builds on our threat-sharing GlobalView network, extensive experience operating security services, and complementary security technologies such as antivirus and APT Detection to provide the highest levels of protection for end users.

GlobalView URL Filtering SDK

CYREN offers embedded URL filtering services, called GlobalView URL Filtering SDK, which can be installed on the partner's machine through SDK. Embedded URL filtering SDK allows us to combat emerging web threats with a URL categorization service designed for maximum security via a global platform with top-rated end user experience based on low-latency, and support for local browsing behaviors.

The vast size of the Internet coupled with the unique browsing habits of individual customers created the need to move the traditional URL database "into the cloud," overcoming local storage limitations and providing customers with information tailored to meet their specific needs.

Embedded URL Filtering works like this:

1. The GlobalView URLF SDK is installed on the partner device (e.g. Web Security Gateway).

2. The partner device receives an http or https request.

3. The device uses the GlobalView SDK to check the URL classification. The GlobalView URLF engine first checks its local cache for URL values; typically more than 99% of queries are locally resolved by the cache.

4. If necessary, the GlobalView URLF engine queries the CYREN Detection and Classification Center for relevant updates.

5. The partner device blocks, allows or strips content according to the classification it receives from the GlobalView URLF engine.

The GlobalView Cloud provides broad, up-to-date coverage of URLs for an end user. CYREN is able to provide high categorization accuracy because of our powerful cloud analysis engines and global data sources. Each SDK installation can include a local cache that automatically customizes itself depending on its usage which allows us to deliver the most relevant data at fast speeds.

CYREN URL Filtering requests between the SDK and the CYREN cloud infrastructure are satisfied in a few milliseconds or less, so latency is not an issue. We employ a combination of deep coverage and highly accurate categorization to ensure the best possible browsing experience for end users.

CYREN Embedded Antivirus

CYREN Antivirus SDK is the result of nearly 20 years of history, experience, and adaptive development by the industry's most capable and well-known engineers. CYREN Antivirus technologies protect millions of users, scan more than 4 billion emails per week, and are trusted by many of the largest software, hardware and Internet services companies.

CYREN Embedded AntiVirus provides broad protection against new and zero-hour threats. Our modular design gives partners industry-leading performance through ultra-low processing, memory, storage, and bandwidth consumption. CYREN Embedded Antivirus SDK offers superior, efficient detection with a small footprint, appropriate for integration into a wide variety of products or services. This award-winning engine blocks malware of all types, including worms, Trojans and spyware. CYREN Embedded Antivirus has been defending against malware for over 20 years.

With CYREN Embedded Antivirus integrated into the vendor device or application, objects (files, web scripts, emails, etc.) are scanned and classified by our antivirus engine. This enables our partners to delete or quarantine these objects and block malicious web scripts before they can impact the end users. CYREN Embedded Antivirus can be deployed within multiple software applications and hardware platforms as diverse as UTMs, Network Attached Storage, Network Routers, and Mobile platforms.

The CYREN Embedded AntiVirus engine uses a modular framework. Each Threat Protection Module within the framework scans specific objects, for example PDF files, or searches for specific virus types (e.g., polymorphic viruses). This architecture is more flexible than the monolithic engines of competitors - new modules can be added quickly to combat new threats without having to change existing ones – giving faster protection from evolving threats.

The modular architecture also means faster deployment for our partners. Quality Assurance testing of the engine is completed far more rapidly after module updates or additions since existing modules are left untouched. We use a minimal number of function calls for integration of the engine, speeding integration time. Also, new features are exposed by adding parameters without changing the basic function call set; ensuring backward compatibility and easier management of deployed product.

CYREN EmailSecurity

Email is by far the largest repository of unstructured data, so the ability to effectively secure email inboxes from unwanted spam and threats like malware and phishing is critical. Today’s preferred delivery model for both providers and customers for this protection is “as-a-service”. CYREN EmailSecurity combines inbound and outbound antispam, antivirus, and virus outbreak detection components in a seamless, easy end user experience. CYREN EmailSecurity uses the CYREN GlobalView™ Cloud, which collects and analyzes billions of transactions per day, to deliver unmatched insight into, and protection against emerging security threats. Our patented Recurrent Pattern Detection (RPD) automatically analyzes collected traffic to provide accurate spam and phishing classifications based on a unique global view of outbreaks

CYREN EmailSecurity frees inboxes of spam, viruses, and phishing threats without blocking important business messages — protecting email users whenever, wherever, and on whatever device they need. CYREN EmailSecurity processes each email message before it enters the end-user's system. If spam or malware is detected, CYREN EmailSecurity handles the message according to the policy defined by the user administrator. All email categorization and reporting details can be viewed in the CYREN EmailSecurity dashboard.

To protect customer privacy, emails are fingerprinted and then only fingerprints are analyzed against the RPD database. In this way, no

sensitive customer data is ever sent to the cloud. If the email is spam, or contains malware it is processed according to the customer's specified business rules, with options such as reject, tag and deliver, reroute, or send to quarantine.

Outbound Anti-Spam

One of the biggest challenges service providers face springs from inside their own infrastructure. Spam attacks emanating from within cause irreparable damage to business and network reputation and customer confidence. Unlike other solutions, CYREN Outbound AntiSpam (OAS) neutralizes this challenge at the source.

CYREN patented Recurrent Pattern Detection technology analyzes and compares email traffic to established local and global patterns, detecting outbound spam within seconds. All malware, spam, or phishing emails found are deleted immediately and a full report detailing their source along with samples of malicious emails is sent to the administrator for remediation.

Sales and Marketing

Our goal is to increase sales to new customers and increase renewals, upgrades and other incremental business to existing customers by expanding our security offerings and increasing the number and productivity of the OEM, distributors and resellers who sell our products to end user customers worldwide.

We sell our products and services internationally in approximately 190 countries primarily through third party distribution channels comprised of distributors and value-added resellers with substantial support from our internal sales team and sales engineers. Generally, our SDK products are 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 virus outbreak detection gateway, CSAM antivirus and F-PROT antivirus services, are sold through resellers, who typically pay us pre-negotiated fees after each sale is closed with a reseller's customer.

As part of our strategy to expand our business to existing customers and to grow sales to channel partners, as well as new customers through expanded market coverage, we increased headcount in our sales force in 2013 and plan to further increase headcount in 2014.

CYREN sales are managed by our Senior Vice President, Worldwide Sales, who is based in our Virginia office and who works closely with our sales teams in the Americas, Europe, Middle East and Africa (EMEA) and Asia Pacific (APAC).

Our marketing efforts are designed to increase recognition of CYREN as a leading provider of cloud-based security solutions that deliver powerful protection through unmatched data intelligence. With our new CYREN brand, we are focused on building brand equity by developing a reputation for easily deployed web, email, and antimalware products that deliver uncompromising protection in both embedded and security-as-a-service deployments. Emphasizing CYREN's cloud-based threat detection and proactive security analytics to provide up-to-date spam classifications, URL categorization and malware detection services helps to define the brand accurately.

We focus our marketing activities on business executives, including product and business development security professionals and, upper level management. We actively manage our public relations programs, communicating directly with security professionals, industry analysts and the media in an effort to promote greater awareness of the growing problems caused by advanced malware attacks, viruses, spam, phishing and ransomware.

Our marketing initiatives include:

- digital advertising promoting CYREN solutions, technologies, partnerships and benefits in security trade magazines and other business-oriented periodicals;
- participating in and sponsorship of trade shows and industry events;
- providing access to the CYREN Security Lab, which informs visitors of real-time security threats;
- conducting webinars and training sessions for our sales organization and partners; and

- utilizing our website and other social media to provide product and company information to our customers and interested parties.

Our Chief Marketing Officer develops and directs the marketing strategy and initiatives from our Virginia office with regionalization accomplished through marketing personnel in our international offices.

Intellectual Property

We regard our patented and patent pending anti-spam and antivirus 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 based on the filing of U.S. Provisional Patent Application. This application remains pending. During 2006, we filed in the United States a provisional 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 that application was then divided into three pending applications. The United States Patent and Trademark Office 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. On May 29, 2012 and on June 5, 2012, two additional divisional patents were issued in connection with the final two split applications – United States Patent No. 8,190,737 and United States Patent No. 8,195,795, respectively, both of which also will have a term concurrent with U.S. Patent 7,849,186. In 2013, we filed in the United States a new application for a patent regarding a unified platform that leverages the various proprietary Internet security tools we employ to resolve security threats. We may seek to patent certain additional software or other technology in the future.

We filed trademark applications for “CYREN”. We are actively maintaining our registered trademark for “Commtouch”, which is registered in the U.S., Canada, Israel, European Union and China. Through acquisition, we also acquired registered trademarks in “FRISK”, “F-PROT”, “eleven”, “Expurgate”, “Command Antimalware” and “Galileo”. We are allowi the registration of Command Interceptor to lapse, and may allow others of these trademarks to lapse over time. 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 commom law trademark rights in “RPD” and “Recurrent Pattern Detection”, as applicable to our messaging security solutions. We have also been claiming common law 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 Internet Protocol, 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. During early 2013, we learned that our customer is negotiating a settlement of the matter, and we contributed a portion towards the settlement.

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.

The propagation of email viruses, whether through email or websites, 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 antivirus industry in general and our Command Antivirus, F-PROT antivirus, Zero-Hour Virus Outbreak Detection and GlobalView URL filtering solutions in particular.

Geographic Information

The Company conducts its business on the basis of one reportable segment.

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 Ended December 31,		
	2011	2012	2013
Israel	$ 2,044	$ 2,541	$ 1,602
North America	12,655	11,847	12,726
Europe	4,869	5,737	14,407
Asia	3,036	3,484	2,717
Other	412	301	796
	$ 23,016	$ 23,910	$ 32,248

Competitive Landscape

The markets in which CYREN competes are intensely competitive and rapidly changing. However, we believe there are very few competitors that offer the complete package of anti-spam, antivirus (both traditional and complementary real-time offerings), IP reputation and web security protections that CYREN 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 and services 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 security providers offering forms of software as a service (SaaS), packaged software (gateway), multi-functional appliances and managed service solutions and which may be viewed as both competitors and potential customers to CYREN include Google (Postini), Symantec (Brightmail), TrendMicro, Intel (McAfee) and Cisco (IronPort), Proofpoint, and Mimecast. Messaging security providers offering solutions on an OEM basis similar to CYREN's business model, and which may be viewed as direct competitors, include Cloudmark, Mailshell and Vade Retro.

The market for real-time virus protection products is also constantly evolving, as those designing and proliferating viruses and other malware seek new vulnerabilities and distribution techniques, and also continue to leverage email distribution as a cost-effective medium for accurately targeting broad, numerous potential victims. CYREN's real-time offering differs from traditional antivirus solutions (such as our Command Antimalware solution) by leveraging our global footprint and patented RPD technology to rapidly detect outbreaks, often hours or days before traditional antimalware solutions; it thereby offers a complementary solution to signature and heuristic-based antivirus engines. For this reason, our Zero-Hour virus outbreak protection engine has been deployed by several security companies and service providers.

In the market for antimalware solutions, there are vendors offering fairly effective solutions using various technologies based on signatures, emulation and heuristics. CYREN has an exclusive OEM/service provider focus, plus an increasing focus on heuristics and zero day effectiveness. Most companies in this space provide end user products and in some cases make software development kits available on an OEM basis. Competitors to CYREN include McAfee, Symantec, Sophos, Kaspersky, and open source software such as Clam-AV.

In the market for web security solutions, there are advanced offerings that compete with our GlobalView URL filtering solution and CWS. Web security 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 CYREN include Intel (McAfee), WebSense, BlueCoat, Zscaler, Barracuda, and Cisco. Web security providers offering solutions on an OEM basis similar to CYREN's business model, and which may be viewed as direct competitors, include Webroot (BrightCloud), Symantec (RuleSpace) and IBM (ISS/Cobion).

We expect that the markets for Internet security solutions will continue to become more consolidated, with companies increasing their presence in this market or entering ancillary markets by acquiring or forming strategic alliances with our competitors or business partners, such as Proofpoint's acquisition of Sendmail and Armorize, IBM's acquisition of Trusteer, Blue Coat's acquisition of Solera, FireEye's acquisition of Mandiant, and Palo Alto's acquisition of Cyvera.

See also disclosure under “Item 3. Key Information– Risk Factors—Business Risks— we face intense competition and could lose market share to our competitors, which could adversely affect our business, financial condition and results of operations."

C. Organizational Structure

The Company wholly owns the following main subsidiary companies, either directly or through holding companies:

a. CYREN Inc., a Delaware corporation and a wholly owned subsidiary of the Company, which has its principal office located at 7925 Jones Branch Drive, Suite 5200, McLean, VA, 22102, tel: (703) 760-3320 where certain members of management and related personnel are located, plus one supporting office located at 1731 Embarcadero Road, Suite 230, Palo Alto, CA 94303, tel: (650) 864–2000.

b. CYREN Iceland hf, a limited liability company organized and existing under the laws of Iceland and wholly owned by the Company, with an office at Thverholti 18, IS-105, Reykjavik, Iceland, tel: 354-540-7400.

c. CYREN Gesellschaft mbH, a German limited liability company owned by the Company through a holding company structure, with an office at Hardenbergplatz 2, 10623, Berlin, Germany, tel: 49 (0)30/52 0056–0.

D. Property, plants and equipment

All of our facilities are leased.

Our office in Herzilya, Israel, is approximately 11,840 square feet and houses research and development, sales, marketing, support and administrative personnel. Our U.S. subsidiary CYREN Inc. is headquartered in McLean, VA in an office of approximately 7,022 square feet and it houses senior management, marketing, sales, and administrative personnel; and its office in California (approximately 3,332 square feet), is staffed by hosting (operations), sales and administrative personnel. Our subsidiary CYREN Iceland hf is located in Reykjavik, Iceland in an office of approximately 10,764 square feet, which houses antivirus operations, sales and some administrative personnel. Our subsidiary CYREN GmbH is based in Berlin, Germany in an office of approximately 10,333 square feet, which houses research and development, operations, sales, marketing and administrative personnel.

Item 4A. Unresolved Staff Comments.

Not applicable.

Item 5. Operating and Financial Review and Prospects.

Overview

From 2003 through 2008, the sole focus of our business had been the development and selling, through reseller and OEM distribution channels, of anti-spam, Zero-Hour virus outbreak detection and IP reputation solutions to a wide array of customers. During late 2008, we expanded our focus by way of the release of our first URL filtering solutions for the web security market. In September 2010, we acquired certain assets comprising the Command Antivirus business unit of Authentium, Inc. On October 1, 2012, the Company completed the acquisition of the antivirus business of Frisk. The acquisition has enabled the Company to provide antivirus technology utilizing the combined resources of both organizations. It has also helped support the launch of a private label antivirus solution for the OEM and service provider markets while also enhancing the Company's SaaS capabilities. On November 16, 2012, the Company completed the acquisition of eleven. The acquisition of eleven has enabled CYREN to accelerate delivery

of private label cloud–based security solutions specifically designed for the OEM and service provider markets.

Critical Accounting Policies and Estimates

This “Item 5. Operating and Financial Review and Prospects” section is based upon the Company’s consolidated financial statements, which have been prepared in accordance with accounting principles generally accepted in the United States (U.S. GAAP). The preparation of these financial statements requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. Actual results could differ from those estimates. On an ongoing basis, the Company's management evaluates estimates. Such estimates are based on historical experience and on various other assumptions that are believed to be reasonable, the results of which form the basis for making judgments about the carrying values of assets and liabilities.

Accounting for Stock–Based Compensation

ASC 718 - "Compensation-Stock Compensation" ASC 718, requires companies to estimate the fair value of equity-based payment awards on the date of grant using an option-pricing model. The value of the portion of the award that is ultimately expected to vest is recognized as an expense over the requisite service periods in the Company's consolidated income statements.

The Company recognizes compensation expense for the value of its awards on a straight line basis over the requisite service period of each of the awards, net of estimated forfeitures. Estimated forfeitures are based on actual historical pre-vesting forfeitures. ASC 718 requires forfeitures to be estimated at the time of grant and revised, if necessary, in subsequent periods if actual forfeitures differ from those estimates.

The Company estimates the fair value of stock options granted using the Black-Scholes option-pricing model. The option-pricing model requires a number of assumptions, of which the most significant are the expected stock price volatility and the expected option term. Expected volatility was calculated based upon actual historical stock price movements. The expected term of options granted represents the period of time that options granted are expected to be outstanding. The risk-free interest rate is based on the yield from U.S. treasury bonds with an equivalent term. The Company has historically not paid dividends and has no foreseeable plans to pay dividends.

The Company applies ASC 718, and ASC 505-50, "Equity Based Payments to Non Employees", or ASC 505-50, with respect to options issued to non-employees.

The fair value for options granted in 2011, 2012 and 2013 is estimated at the date of grant using a Black-Scholes options pricing model with the following weighted average assumptions:

	Year ended December 31,		
Employee stock options	2011	2012	2013
Volatility	68%-70 %	38%-51 %	37%-47 %
Risk-free interest rate	0.6%-2.1%	0.5%-0.9%	0.5%-1.5%
Dividend yield	0 %	0 %	0 %
Expected life (years)	3.6-4.8	3.8-4.9	3.5-4.9

Revenue Recognition

The Company derives its revenues from the delivery of real-time cloud-based services for each of the email security, web-filtering, and antimalware offerings.

Revenue is recognized when there is a persuasive evidence of an arrangement, the service has been rendered, the collection of the fee is probable and the amount of fees to be paid by the customer is fixed or determinable.

Revenues from such services are recognized ratably over the contractual service term, which generally includes a term period of one to three years.

Deferred revenues include unearned amounts received from customers, but not yet recognized as revenues.

Accounting for Income Tax

We account for income taxes in accordance with FASB ASC 740, "Income Taxes." ASC 740 prescribes the use of the liability method whereby deferred tax assets and liability account balances are determined based on differences between financial reporting and tax bases of assets and liabilities and are measured using the enacted tax rates and laws that will be in effect when the differences are expected to reverse. We record a valuation allowance to reduce deferred tax assets to the amount that we believe is more likely than not to be realized.

Deferred tax assets are classified as current or non-current based on the classification of the related asset or liability for financial reporting, or according to the expected reversal dates of the specific temporary differences if not related to an asset or liability for financial reporting.

ASC 740 contains a two-step approach to recognizing and measuring a liability for uncertain tax positions. The first step is to evaluate the tax position taken or expected to be taken in a tax return by determining if the weight of available evidence indicates that it is more likely than not that, on an evaluation of the technical merits, the tax position will be sustained on audit, including resolution of any related appeals or litigation processes. The second step is to measure the tax benefit as the largest amount that is more than 50% likely to be realized upon ultimate settlement. No liability for unrecognized tax benefits was recorded as a result of the implementation of ASC 740.

Goodwill and Intangible Assets

Goodwill and certain other purchased intangible assets have been recorded as a result of acquisitions made in 2010 and 2012. Goodwill represents the excess of the purchase price in a business combination over the fair value of net tangible and intangible assets acquired. Goodwill is not amortized, but rather is subject to an impairment test. The Company performs an annual impairment test at December 31 of each fiscal year, or more frequently if impairment indicators are present. We operate in one operating segment, and this segment comprises the only reporting unit.

ASC 350 prescribes a two-phase process for impairment testing of goodwill. The first phase screens for impairment, while the second phase (if necessary) measures impairment. Goodwill impairment is deemed to exist if the net book value of a reporting unit exceeds its estimated fair value determined using market capitalization. In such case, the second phase is then performed, and the Company measures impairment by comparing the carrying amount of the reporting unit's goodwill to the implied fair value of that goodwill. An impairment loss is recognized in an amount equal to the excess. ASC 350 allows an entity to first assess qualitative factors to determine whether it is necessary to perform the two-step quantitative goodwill impairment test. An entity is not required to calculate the fair value of a reporting unit unless the entity determines, based on a qualitative assessment, that it is more likely than not that its fair value is less than its carrying amount.

Alternatively, ASC 350 permits an entity to bypass the qualitative assessment for any reporting unit and proceed directly to performing the first step of the goodwill impairment test.

The Company performs an annual impairment test at December 31, of each fiscal year, or more frequently if impairment indicators are present. The Company operates in one operating segment, and this segment comprises its only reporting unit.

During 2012 and 2013, no impairment losses have been identified. In 2011, impairment losses of $502 thousand were recorded in respect of covenants not to compete.

Intangible assets that are not considered to have an indefinite useful life are amortized over their estimated useful lives, which range from 8 to 15 years. Acquired customer contracts and relationships are amortized over their estimated useful lives in proportion to the economic benefits realized. This accounting policy results in accelerated amortization of such customer contracts and relationships arrangements as compared to the straight-line method. Other intangible assets consist primarily of technology, and are amortized over their estimated useful lives on a straight-line basis.

The carrying amount of these assets to be held and used is reviewed whenever events or changes in circumstances indicate that the carrying value of an asset may not be recoverable. Recoverability of these assets is measured by comparison of the carrying amount of each asset group to the future undiscounted cash flows the asset group is expected to generate. If the asset is considered to be impaired, the amount of any impairment is measured as the difference between the carrying value and the fair value of the impaired asset.

During 2012 and 2013, no impairment losses have been identified. In 2011, impairment losses of $502 thousand were recorded in respect of covenants not to complete.

Fair Value Measurements

The carrying amounts of cash and cash equivalents, trade receivables, prepaid expenses, other receivables and trade payables, approximate their fair values due to the short-term maturities of such financial instruments.

The Company measures its earn-out consideration at fair value. Fair value is an exit price, representing the amount that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants. As such, fair value is a market-based measurement that should be determined based on assumptions that market participants would use in pricing an asset or a liability. A three-tier fair value hierarchy is established as a basis for considering such assumptions and for inputs used in the valuation methodologies in measuring fair value:

· Level 1 - Quoted prices (unadjusted) in active markets for identical assets or liabilities that the Company can access at the measurement date.

· Level 2 - Inputs other than quoted prices included within Level 1 that are observable for the asset or liability, either directly or indirectly.

· Level 3 - Unobservable inputs for the asset or liability.

The availability of observable inputs can vary from instrument to instrument and is affected by a wide variety of factors, including, for example, the type of instrument, the liquidity of markets and other characteristics particular to the transaction. To the extent that valuation is based on models or inputs that are less observable or unobservable in the market, the determination of fair value requires more judgment and the instruments are categorized as Level 3.

The fair value hierarchy also requires an entity to maximize the use of observable inputs and minimize the use of unobservable inputs when measuring fair value.

The Company's earn-out considerations are classified within Level 3. The valuation methodology used by the Company to calculate the fair value of the earn-out considerations is the discounted cash-flow method. The assumptions used in the valuation of the earn-out considerations as of December 31, 2013 included forecasted undiscounted future cash-flows and a weighted average cost of capital of 18.3% related to the earn-out originating from the Frisk acquisition and 16.4% related to the earn-out originating from the eleven acquisition.

A. Operating results

Results of Operations

The following table sets forth financial data for the years ended December 31, 2011, 2012 and 2013 (in thousands):

	2011	2012	2013
Revenues	$23,016	$23,910	$32,248
Cost of revenues	4,091	4,350	7,201
Gross profit	18,925	19,560	25,047
Operating expenses:			
Research and development, net	5,410	6,281	9,156
Sales and marketing	5,486	5,860	10,886
General and administrative	4,721	6,639	10,388
Adjustment to earnout consideration	-	-	(3,276)
Total operating expenses	15,617	18,780	27,154
Operating income (loss)	3,308	780	(2,107)
Loss from sale of investment in affiliate	-	-	(1,289)
Financial income (expense), net	(27)	80	(1,255)
Income (loss) before taxes on income	3,281	860	(4,651)
Tax benefit (expense)	1,317	625	(5,220)

Net income (loss)	$4,598	$1,485	$(9,871)

Comparison of Years Ended December 31, 2013 and 2012

Revenues. Revenues for 2013 increased by $8.3 million from $23.9 million in 2012 to $32.2 million in 2013, which represents a 35% increase. The increase is mainly due to a full year of revenue from the 2012 fourth quarter acquisition and the consolidation of eleven and Frisk.

Cost of Revenues. Cost of revenues increased by $2.8 million from $4.4 million in 2012 to $7.2 million in 2013, which represents a 66% increase. The increase in 2013 is mainly due to the full year consolidation of eleven and Frisk into the Company. These increases include higher facility costs and hosting expenses aimed to serve the increasing number of our customers, intangible amortization, certain fees, and payroll costs.

Research and Development, Net. Research and development expenses increased by $2.9 million and amounted to $9.2 million in 2013 compared to $6.3 million in 2012. The increase was mainly due to the full year consolidation of eleven and Frisk. Payroll and related expenses increased primarily due to the manpower investment related to two significant product development launches, CYREN Web Security (CWS) and Advanced Persistent Threat (APT). Research and development expenses also include $0.3 million of expenses for equity based compensation, compared to $0.2 million of expenses in 2012.

Sales and Marketing. Sales and marketing expenses increased by $5.0 million and amounted to $10.9 million in 2013, compared to $5.9 million in 2012. The increase is due in part to the full year consolidation of eleven and Frisk compared to a partial fourth quarter of expenses in 2012. The increase includes intangible amortization, payroll costs due to the Company’s focus on growth, and rebranding. Sales and marketing expenses in 2013 included $0.3 million expenses in connection with equity based compensation, compared to $0.2 million of expenses in 2012.

General and Administrative. General and administrative expenses increased by $3.8 million, from $6.6 million in 2012 to $10.4 million in 2013. $1.7 million of the total increase is due to the full year consolidation of eleven and Frisk. Payroll and related costs increased over 2012 partially due to the migration of some of the management functions to the U.S. headquarters and the investment in senior management, including related recruiting expenses, to support the future growth of the Company. Rent and occupancy costs also increased due to office relocation in Israel, Virginia and California, and improvements to the facilities. In 2012 there were $0.8 million of acquisition related costs of eleven and Frisk. In 2013, general and administrative expenses included $0.8 million expenses in connection with equity based compensation, compared to $0.8 million of expenses in 2012.

Loss from Sale of Investment in Affiliate. In 2013, the Company sold its investment in its affiliate for a consideration of $194 thousand and recognized a loss from sale of investment of $1,289 thousand as of December 31, 2013.

Financial Income (Expense), Net. Financial income (expenses), net, resulted in net expenses in the amount of $1.3 million compared to income of $0.08 million in 2012. In 2013, $0.9 million is related to the earnout accretion for eleven and Frisk compared to $0.2 million in 2012.

Tax Benefit (Expense). Tax benefit decreased by $5.8 million from $0.6 million in 2012 to a tax expense of $5.2 million in 2013. Management currently believes that based upon its estimations for future taxable income, it is more likely than not that the deferred tax assets regarding the loss carryforwards will not be utilized in the foreseeable future. Thus, a valuation allowance was provided to reduce deferred tax assets to their realizable value. As a result, in 2013, we recorded an adjustment to the deferred tax assets and liabilities of $5.0 million. In addition, current taxes of $0.2 million were recorded on account of the Company's German subsidiary.

Comparison of Years Ended December 31, 2012 and 2011

Revenues. Revenues increased by $0.9 million from $23.0 million in 2011 to $23.9 million in 2012, which represents a 4% increase. The increase is mainly due to the acquisition and the first consolidation of eleven and Frisk into CYREN in the fourth quarter of 2012.

Cost of Revenues. Cost of revenues increased by $0.3 million from $4.1 million in 2011 to $4.4 million in 2012, which represents a 6% increase. The increase in 2012 is mainly due to the first consolidation of eleven and Frisk into CYREN as well as higher facility costs and hosting expenses aimed to serve the increasing number of customers.

Research and Development, Net. Research and development expenses increased by $0.9 million and amounted to $6.3 million in 2012 compared to $5.4 million in 2011. $0.7 million out of the total increase is due to the first consolidation of eleven and Frisk in the fourth quarter of 2012 and $0.2 million out of the total increase is due to increase in outside services utilized in 2012. Research and development expenses in 2012 include $0.2 million of expenses in connection with equity based compensation, compared to $0.3 million of expenses in 2011.

Sales and Marketing. Sales and marketing expenses increased by $0.4 million and amounted to $5.9 million in 2012, compared to $5.5 million in 2011. The increase is partly due to the first consolidation of Frisk and eleven in the fourth quarter of 2012. Excluding eleven and Frisk, Sales and Marketing payroll increased by $0.3 million in order to expand our existing sales and product marketing resources and rent increased by $0.2 million due to the opening of the new headquarters in Virginia. This increase is offset by a decrease of $0.5 million due to the write off in 2011 of a covenant not to compete asset (acquired in our Authentium acquisition). Sales and marketing expenses in 2012 included $0.2 million expenses in connection with equity based compensation, compared to $0.4 million of expenses in 2011.

General and Administrative. General and administrative expenses increased by $1.9 million, from $4.7 million in 2011 to $6.6 million in 2012. Of the total increase, $0.8 million is due to acquisition related costs of eleven and Frisk. Salary expenses increased by $0.7 million from $2.8 million in 2011 to $3.5 million in 2012 mainly due to recruitment of additional employees in the Virginia headquarters. Additionally, $0.3 million is due to the first consolidation of Frisk and eleven in the fourth quarter of 2012.

In 2012, general and administrative expenses included $0.8 million expenses in connection with equity based compensation, compared to $0.7 million of expenses in 2011.

Financial Income (Expenses), Net. Financial income (expenses), net, resulted in income of $0.08 million in 2012 compared to expenses of $0.03 million in 2011.

Tax Benefit. Tax benefit decreased by $0.7 million from $1.3 million in 2011 to $0.6 million in 2012. In 2012, the deferred tax asset increased by $0.7 million due to an increase in forecasted taxable income that is more likely than not to be realized in the foreseeable future, based on our established pattern of profitability in the last few years resulting, among others, from the new acquisitions that took place in 2012.

Quarterly Results of Operations (Unaudited).

The following table sets forth certain unaudited quarterly statements of operations data for the eight quarters ended December 31, 2013. This information has been derived from the Company's consolidated unaudited financial statements, which, in management's opinion, have been prepared on the same basis as the audited consolidated financial statements, and include all adjustments, consisting only of normal recurring adjustments, necessary for a fair presentation of the information for the quarters presented. This information should be read in conjunction with our audited consolidated financial statements and the notes thereto included elsewhere in this Annual Report. The operating results for any quarter are not necessarily indicative of the operating results for any future period.

	Three Months Ended							
(in thousands of U.S. dollars) (unaudited)	Mar 31 2012	Jun 30 2012	Sep 30 2012	Dec 31 2012	Mar 31 2013	Jun 30 2013	Sep 30 2013	Dec 31 2013
Revenues	$5,896	$5,671	$5,558	$6,785	$7,925	$8,055	$8,019	$8,249
Cost of revenues	1,052	1,014	917	1,367	1,778	1,756	1,722	1,945
Gross profit	4,844	4,657	4,641	5,418	6,147	6,299	6,297	6,304
Operating expenses:								
Research and development, net	1,270	1,364	1,462	2,185	2,264	2,182	2,079	2,631
Sales and marketing	1,142	1,288	1,564	1,866	2,765	2,537	2,559	3,025
General and administrative	1,331	1,384	1,550	2,374	2,216	2,263	2,112	3,797
Adjustment to earnout consideration	-	-	-	-	-	-	-	(3,276)
	3,743	4,036	4,576	6,425	7,245	6,982	6,750	6,177

Total operating expenses								
Operating income (loss)	1,101	621	65	(1,007)	(1,098)	(683)	(453)	127
Loss from sale of investment in affiliate	-	-	-	-	-	-	-	(1,289)
Financial income (expense), net	23	64	63	(70)	(184)	(358)	(323)	(390)
Income (loss) before taxes on income	1,124	685	128	(1,077)	(1,282)	(1,041)	(776)	(1,552)
Tax benefit (expense)	85	119	(109)	530	23	296	(138)	(5,401)
Net income (loss)	$1,209	$804	$19	$(547)	$(1,259)	$(745)	$(914)	$(6,953)
Basic Net income (loss) per share	$0.05	$0.03	$0.00	$(0.02)	$(0.05)	$(0.03)	$(0.03)	$(0.26)
Diluted net income (loss) per share	$0.05	$0.03						