

CyberArk Software Ltd.  
Form 424B4  
June 11, 2015  
Table of Contents

**Prospectus**

**Filed pursuant to Rule 424(b)(4)  
Registration No. 333-204516**

**4,900,000 Shares**

**Ordinary Shares**

We are offering 900,000 ordinary shares and the selling shareholders are offering an additional 4,000,000 ordinary shares. We will not receive any of the proceeds from the sale of the shares being offered by the selling shareholders.

Our ordinary shares are listed on the NASDAQ Global Select Market under the symbol **CYBR** . On June 10, 2015, the last reported sales price of our ordinary shares was \$63.37 per share.

	<b>Per Share</b>	<b>Total</b>
Public offering price	\$ 61.00	\$ 298,900,000
Underwriting discounts and commissions(1)	\$ 2.44	\$ 11,956,000
Proceeds to us (before expenses)	\$ 58.56	\$ 52,704,000
Proceeds to the selling shareholders (before expenses)	\$ 58.56	\$ 234,240,000

(1) See **Underwriting (Conflicts of Interest)** for a description of compensation payable to the underwriters. The selling shareholders have granted the underwriters an option to purchase up to 735,000 additional ordinary shares from the selling shareholders, at the public offering price, less the underwriting discount, for 30 days after the date of this prospectus.

**We are an emerging growth company as defined under the federal securities laws and, as such, may elect to comply with certain reduced public company reporting requirements.**

**Investing in our ordinary shares involves a high degree of risk. See Risk Factors beginning on page 12.**

Neither the Securities and Exchange Commission nor any state securities commission has approved or disapproved of these securities or determined if this prospectus is truthful or complete. Any representation to the contrary is a criminal offense.

The underwriters expect to deliver the ordinary shares to purchasers on or about June 16, 2015.

<b>Goldman, Sachs &amp; Co.</b>	<b>Deutsche Bank Securities</b>	<b>Barclays</b>	<b>BofA Merrill Lynch</b>	<b>UBS Investment Bank</b>
<b>William Blair</b>		<b>Nomura</b>		<b>Oppenheimer &amp; Co.</b>
		<b>June 10, 2015</b>		

**Table of Contents****TABLE OF CONTENTS**

	<b>Page</b>
<u>Summary</u>	1
<u>Risk Factors</u>	12
<u>Special Note Regarding Forward-Looking Statements</u>	33
<u>Market and Industry Data</u>	34
<u>Use of Proceeds</u>	35
<u>Price Range of our Ordinary Shares</u>	36
<u>Dividend Policy</u>	37
<u>Capitalization</u>	38
<u>Dilution</u>	39
<u>Selected Consolidated Financial Data</u>	40
<u>Management's Discussion and Analysis of Financial Condition and Results of Operations</u>	43
<u>Business</u>	66
<u>Management</u>	85
<u>Principal and Selling Shareholders</u>	111
<u>Certain Relationships and Related Party Transactions</u>	114
<u>Description of Share Capital</u>	116
<u>Shares Eligible for Future Sale</u>	121
<u>Taxation and Israeli Government Programs Applicable to Our Company</u>	123
<u>U.S. and Israeli Tax Consequences for Our Shareholders</u>	127
<u>Underwriting (Conflicts of Interest)</u>	134
<u>Legal Matters</u>	141
<u>Experts</u>	142
<u>Enforceability of Civil Liabilities</u>	143
<u>Where You Can Find Additional Information</u>	144
<u>Index to Consolidated Financial Statements</u>	F-1

Neither we, the selling shareholders nor the underwriters have authorized anyone to provide information different from that contained in this prospectus, any amendment or supplement to this prospectus or in any free writing prospectus prepared by us or on our behalf. Neither we, the selling shareholders nor the underwriters take any responsibility for, and can provide no assurance as to the reliability of, any information other than the information in this prospectus and any free writing prospectus prepared by us or on our behalf. Neither the delivery of this prospectus nor the sale of our ordinary shares means that information contained in this prospectus is correct after the date of this prospectus. This prospectus is not an offer to sell or the solicitation of an offer to buy these ordinary shares in any circumstances under which such offer or solicitation is unlawful.

(i)

**Table of Contents**

**SUMMARY**

*This summary highlights selected information contained elsewhere in this prospectus. This summary does not contain all the information that you should consider before deciding to invest in our ordinary shares. You should read the entire prospectus carefully, including Risk Factors and our consolidated financial statements and notes to those consolidated financial statements, before making an investment decision. In this prospectus, the terms CyberArk, we, us, our and the company refer to CyberArk Software Ltd. and its subsidiaries.*

**Overview**

We are a global leader and pioneer of a new layer of IT security solutions that protects organizations from cyber attacks that have made their way inside the network perimeter to strike at the heart of the enterprise. Our software solution is focused on protecting privileged accounts, which have become a critical target in the lifecycle of today's cyber attacks. Privileged accounts are pervasive and act as the keys to the IT kingdom, providing complete access to, and control of, all parts of IT infrastructure, industrial control systems and critical business data. In the hands of an external attacker or malicious insider, privileged accounts allow attackers to take control of and disrupt an organization's IT and industrial control infrastructures, steal confidential information and commit financial fraud. Our comprehensive solution proactively protects privileged accounts, monitors privileged activity and detects malicious privileged behavior. Our customers use our innovative solution to introduce this new security layer to protect against, detect and respond to cyber attacks before they strike vital systems and compromise sensitive data.

Organizations worldwide are experiencing an unprecedented increase in the sophistication, scale and frequency of cyber attacks. The challenge this presents is intensified by the growing adoption of new technologies, such as cloud computing, virtualization, software-defined networking, enterprise mobility and social networking, which has resulted in increasingly complex and distributed IT environments with significantly larger attack surfaces. Organizations have historically relied upon perimeter-based threat protection solutions such as network, web and endpoint security tools as the predominant defense against cyber attacks, yet these traditional solutions have a limited ability to stop today's advanced threats. As a result, an estimated 90% of organizations have suffered a cybersecurity breach according to a 2011 survey of approximately 580 U.S. IT practitioners by the Ponemon Institute, a research center focused on privacy, data protection and information security policy. Organizations are just beginning to adapt their security strategies to address this new threat environment and are evolving their approaches based on the assumption that their network perimeter has been or will be breached. They are therefore increasingly implementing new layers of security inside the network to disrupt attacks before they result in the theft of confidential information or other serious damage. Regulators are also continuing to mandate rigorous new compliance standards and audit requirements in response to this evolving threat landscape.

We believe that the implementation of a privileged account security solution is one of the most critical layers of an effective security strategy. Privileged accounts represent one of the most vulnerable aspects of an organization's IT infrastructure. Privileged accounts are used by system administrators, third-party and cloud service providers, applications and business users, and they exist in nearly every connected device, server, hypervisor, operating system, database, application and industrial control system. Due to the broad access and control they provide, exploiting privileged accounts has become a critical stage of the cyber attack lifecycle. The typical cyber attack involves attackers effecting an initial breach, escalating privileges to access target systems, moving laterally through the IT infrastructure to identify valuable targets, and exfiltrating, or stealing, the desired information. According to Mandiant, credentials of authorized users were hijacked in 100% of the breaches that Mandiant investigated, and privileged accounts were targeted whenever possible.



## Table of Contents

We have architected our solution from the ground up to address the challenges of protecting privileged accounts and an organization's sensitive information. Our solution provides proactive protection against cyber attacks from both external and internal sources and allows for real-time detection and neutralization of such threats. It can be deployed in traditional on-premise data centers, cloud environments and industrial control systems. Our innovative software solution is the result of over 15 years of research and expertise, combined with valuable knowledge we have gained from working with our diverse population of customers.

Our Privileged Account Security Solution is built on our shared technology platform and consists of several products:

*Enterprise Password Vault:* proactively protects and manages all privileged accounts across an entire organization

*SSH Key Manager:* securely stores, rotates and controls access to SSH keys to prevent unauthorized access to privileged accounts

*Privileged Session Manager:* enables live monitoring and command-line keystroke level recording of privileged sessions, isolates the target asset from malware and establishes a single point of control for all privileged activity

*Application Identity Manager:* secures application to application interfaces by enabling proactive controls on privileged credentials embedded in applications, service accounts and scripts

*On-Demand Privileges Manager:* limits the breadth of access of administrative accounts by restricting the use of specified commands and functions

*Privileged Threat Analytics:* profiles and analyzes individual privileged user behavior and creates prioritized alerts when abnormal activity is detected

As of March 31, 2015, we had approximately 1,850 customers, including approximately 40% of the Fortune 100 and approximately 18% of the Global 2000. We define a customer to include a distinct entity, division or business unit of a company. Our customers include leading enterprises in a diverse set of industries, including energy and utilities, financial services, healthcare, manufacturing, retail, technology and telecommunications, as well as government agencies. We sell our solution through a high touch, channel fulfilled hybrid sales model that combines the leverage of channel sales with the account control of direct sales, and therefore provides us with significant opportunities to grow our current customer base. This approach allows us to maintain close relationships with our customers and benefit from the global reach of our channel partners. Additionally, we are enhancing our product offerings and go-to-market strategy by establishing technology alliances within the IT infrastructure and security vendor ecosystem.

Our business has rapidly grown in recent years. During 2012, 2013 and 2014, our revenues were \$47.2 million, \$66.2 million and \$103.0 million, respectively, representing year-over-year growth of 40.1% and 55.7% in 2013 and 2014, respectively. Our net income for 2012, 2013 and 2014 was \$7.9 million, \$6.6 million and \$10.0 million, respectively. Our revenues for the three months ended March 31, 2014 and 2015 were \$17.4 million and \$32.9 million,

respectively, representing year-over-year growth of 89.2%. Our net income for the three months ended March 31, 2015 was \$4.2 million compared with a net loss of \$1.2 million for the same period in 2014.

### **Industry Overview**

The recent increase in sophisticated, targeted security threats by both external attackers and malicious insiders, along with an increase in the attack surface due to the growing complexity and distributed nature of IT environments, have made it extremely challenging for enterprises and governments around the world to protect their sensitive information. These challenges are driving the need for a new layer of security that complements traditional threat protection technologies by securing access to privileged accounts and preventing the exploitation of organizations' critical systems and data.



## **Table of Contents**

Privileged accounts represent one of the most vulnerable aspects of an organization's IT infrastructure. Privileged escalation is a critical stage of the cyber attack because, if privileged credentials are compromised, the attacker is able to move closer to sensitive data while remaining undetected. Today's advanced cyber attacks are typically designed to evade traditional threat prevention technologies that are focused on protecting the perimeter from outside breach. Furthermore, compliance requirements continue to become more stringent in response to the complex and evolving threat landscape.

### **Challenges in Protecting Privileged Accounts**

The increasing sophistication, scale and frequency of advanced cyber attacks challenge traditional cybersecurity methods and create a need for a comprehensive approach to securing privileged accounts from use by external or internal attackers to gain access to and exploit an organization's confidential data and IT systems. Such an approach must address a range of challenges presented by privileged accounts, including:

traditional security solutions' limited ability to protect privileged credentials and critical assets from cyber attacks;

insufficient visibility and lack of automation in the management of privileged accounts;

inability to monitor and audit all privileged activity;

inadequate or delayed response time in detecting malicious and high risk behaviors; and

limited scalability of existing point solutions.

### **Our Solution**

Our Privileged Account Security Solution provides organizations with the following benefits:

***Comprehensive platform for proactive protection of privileged credentials and target assets from cyber attacks.*** Our comprehensive solution for privileged account security enables our customers to proactively protect against and automatically detect and respond to in-progress cyber attacks before they strike vital systems and compromise sensitive data. Our unified solution to these previously disparate security needs enables our customers to preemptively remediate vulnerabilities and improve their security effectiveness from a central command and control point.

***Automatic identification and understanding of the scope of privileged account risk.*** Our solution automatically detects privileged accounts across the enterprise and helps customers visualize the resulting compliance gaps and security vulnerabilities. This automated process reduces the time-consuming and error-prone task of manually tracking and updating privileged credentials, thereby decreasing IT operational

costs. This enhanced visibility significantly improves the security posture of our customers and facilitates adherence to rigorous audit and compliance standards.

***Continuous monitoring, recording and secure storage of privileged account activity.*** Our solution monitors, collects and records individual privileged session activity down to every mouse click and keystroke. It also provides highly secure storage of privileged session recordings, robust search capabilities and full forensics records to facilitate a more rapid and precise response to malicious activity.

***Real-time detection, alerting and response to malicious privileged activity.*** Our Privileged Threat Analytics product uses proprietary algorithms to profile and analyze individual privileged user behavior and creates prioritized alerts in real-time when abnormal activity is detected. This allows our customers' incident response teams to investigate and prioritize threatening activity and respond by terminating the active session.

## **Table of Contents**

***Purpose-built solution, architected for privileged account security.*** Our Digital Vault offers multiple layers of security including robust segregation of duties, a secure proprietary communications protocol and military-grade encryption. Our Privileged Session Manager product establishes a single point of control for all privileged activity, effectively decreasing the attack surface by providing only proxy-based access to IT assets through our platform.

***Scalable and flexible platform that enables modular deployment.*** Our solution is scalable and flexible to enable deployment in large-scale distributed environments for on-premise, cloud environments and industrial control systems. Our solution enables enterprises to leverage their existing investments with out of the box support for many devices, networks, applications and servers, including web sites and social media.

### **Our Market Opportunity**

We believe that the security market is in the midst of a significant transition as enterprises are investing in a new generation of security solutions to help protect them against today's sophisticated and targeted cyber threats from both external attackers and malicious insiders. Gartner estimates that by 2020, 60% of enterprise information security budgets will be allocated to rapid detection and response approaches, up from less than 10% in 2014. Recognizing that traditional perimeter-based threat protection solutions are not sufficient to protect against today's advanced cyber threats, enterprises are investing in security solutions within the datacenter to protect the inside of their networks. According to a 2012 report by International Data Corporation (IDC), worldwide spending on datacenter security solutions was \$10.7 billion in 2011 and is expected to grow to \$16.5 billion by 2016, representing a compound annual growth rate of 9.3%. According to the same report, worldwide spending for IT security solutions was \$28.4 billion in 2011 and is expected to grow to \$40.8 billion in 2016, representing a compound annual growth rate of 7.6%.

We believe that privileged account security is a new, critical layer of security that is benefitting from this transition. Privileged accounts represent one of the most vulnerable aspects of an organization's IT infrastructure and exist in nearly every connected device, server, hypervisor, operating system, database, application and industrial control system throughout on-premise and cloud-based datacenters. As a result, we believe that an increasing portion of the IT security budget, and specifically datacenter security spend, will be allocated for privileged account security solutions.

### **Our Competitive Strengths**

Our mission is to protect the heart of the enterprise from advanced cyber attacks. We have established a leadership position in protecting high-value data and critical IT assets by securing privileged accounts, and have several key competitive strengths including:

***Trusted expert in privileged account security.*** We are a recognized brand name and a leader in privileged account security, protecting organizations worldwide against external threats that have already penetrated the perimeter, as well as threats that originate from within the perimeter by malicious or careless insiders.

***Technology leader driven by vision and focus on innovation.*** Our history of innovation is the cornerstone of our technology leadership. We pioneered Digital Vault technology and introduced patented technology for application identity management, secure connectivity for remote vendors, integrated privileged activity monitoring, private and public cloud privileged account management and privileged threat analytics.

***Global reach driven by direct and indirect sales organization.*** We have a broadly dispersed global hybrid sales channel as evidenced by our existing customer implementations in 65 countries, a broad network of over 200 channel and technology alliance partners worldwide, and local presence in more than 20 countries.

## **Table of Contents**

***Strong management team with significant IT security expertise.*** We have a highly talented management team and a strong research and development organization with significant IT security expertise from past experience in leading IT security companies and Israel's military technology units.

***Corporate culture committed to our customers' success.*** Our commitment to our customers' success is ingrained in our business strategy and is brought to life through constant customer interactions, employee functions and our engaging annual customer conferences attended by hundreds of customers and channel partners.

## **Our Growth Strategy**

Our goal is to be the global leader in IT security solutions that protect organizations from cyber attacks that have made their way inside the network perimeter to strike at the heart of the enterprise. The key elements of our strategy to extend our global leadership include:

continue innovating and enhancing our solution;

growing our customer base;

further penetrating our existing customer base;

continuing to expand our global presence by leveraging systems integrators and distribution partnerships;  
and

selectively pursuing strategic transactions.

## **Risks Associated With Our Business**

Investing in our ordinary shares involves risks. You should carefully consider the risks described in Risk Factors beginning on page 12 before making a decision to invest in our ordinary shares. If any of these risks actually occur, our business, financial condition or results of operations would likely be materially adversely affected. In such case, the trading price of our ordinary shares would likely decline, and you may lose all or part of your investment. The following is a summary of some of the principal risks we face:

The IT security market is rapidly evolving within the increasingly challenging cyber threat landscape. If the industry does not continue to develop as we anticipate, our sales will not grow as quickly as expected and our share price could decline.

If we fail to effectively manage our growth, our business and operations will be negatively affected, and as we invest in the growth of our business, we expect our operating and net profit margins to decline in the

near-term.

Our quarterly results of operations may fluctuate for a variety of reasons, including our failure to close significant sales before the end of a particular quarter.

Our reputation and business could be harmed based on real or perceived shortcomings, defects or vulnerabilities in our solution or the failure of our solution to meet customers' expectations.

If we are unable to acquire new customers, our future revenues and operating results will be harmed.

If we are unable to sell additional products and services to our existing customers, our future revenues and operating results will be harmed.

We face intense competition from IT security vendors, some of which are larger and better known than we are, and we may lack sufficient financial or other resources to maintain or improve our competitive position.

**Table of Contents**

If our internal network system is compromised by cyber attackers or other data thieves, public perception of our products and services will be harmed.

**Corporate Information**

We are incorporated under the laws of the State of Israel. Our principal executive offices are located at 94 Em-Ha moshavot Road, Park Ofer, P.O. Box 3143, Petach Tikva 4970602, Israel, and our telephone number is +972 (3) 918-0000. Our website address is [www.cyberark.com](http://www.cyberark.com). Information contained on, or that can be accessed through, our website does not constitute a part of this prospectus and is not incorporated by reference herein. We have included our website address in this prospectus solely for informational purposes. Our agent for service of process in the United States is Cyber-Ark Software, Inc., located at 60 Wells Avenue, Suite 103, Newton, MA 02459, and our telephone number is (617) 965-1544.

Throughout this prospectus, we refer to various trademarks, service marks and trade names that we use in our business. The CyberArk design logo is the property of CyberArk Software Ltd. CyberArk is our registered trademark in the United States. We have several other trademarks, service marks and pending applications relating to our products. In particular, although we have omitted the ® and trademark designations in this prospectus from each reference to Cyber-Ark DNA, Inter-Business Vault, Network Vault, Password Vault, Privileged Session Manager and Vaulting Technology, all rights to such trademarks are nevertheless reserved. Other trademarks and service marks appearing in this prospectus are the property of their respective holders.

**Table of Contents**

**The Offering**

Ordinary shares offered by us 900,000 ordinary shares

Ordinary shares offered by the selling  
shareholders 4,000,000 ordinary shares

Ordinary shares to be outstanding after this  
offering 31,657,908 ordinary shares

Underwriters' option The selling shareholders have granted the underwriters an option for a period of 30 days after the date of this prospectus to purchase up to 735,000 additional ordinary shares.

Use of proceeds We estimate that the net proceeds to us from this offering will be approximately \$52.0 million, after deducting the underwriting discount and estimated offering expenses. We intend to use the net proceeds for general corporate purposes, including sales and marketing expenditures aimed at growing our business and research and development expenditures focused on product development. We may also use net proceeds to make acquisitions or investments in complementary companies or technologies. Consistent with our growth strategy, we are currently engaged in discussions, negotiations and diligence evaluations with respect to possible acquisitions, although we do not have any agreement or understanding with respect to any material acquisition or investment at this time.

We will not receive any of the proceeds from the sale of ordinary shares by the selling shareholders.

See Use of Proceeds, Principal and Selling Shareholders and Underwriting (Conflicts of Interest).

Risk factors See Risk Factors and other information included in this prospectus for a discussion of factors you should carefully consider before deciding to invest in our ordinary shares.

NASDAQ Global Select Market symbol CYBR

Conflicts of interest Goldman, Sachs & Co. and/or its affiliates own in the aggregate in excess of 10% of our issued and outstanding ordinary shares. As a result,



Goldman, Sachs & Co. is deemed to have a conflict of interest with us within the meaning of Rule 5121 of the Financial Industry Regulatory Authority ( Rule 5121 ). Accordingly, this offering will be made in compliance with the applicable provisions of Rule 5121. In accordance with that rule, the appointment of a qualified independent underwriter is not required in connection with this offering because a bona fide public market exists for our ordinary shares. Any underwriter that has a conflict of interest pursuant to Rule 5121 will not confirm sales to accounts in which it

**Table of Contents**

exercises discretionary authority without the prior written consent of the customer. See Underwriting (Conflicts of Interest).

The number of ordinary shares to be outstanding after this offering and, unless otherwise indicated, the information in this prospectus are based on 30,757,908 ordinary shares outstanding as of March 31, 2015 and excludes 5,144,755 ordinary shares reserved for issuance under our equity incentive plans as of March 31, 2015, of which there were outstanding options to purchase 4,338,682 shares at a weighted average exercise price of \$2.93 per share and 43,040 unvested restricted stock units, or RSUs. In addition, our shareholders have approved at our annual general meeting of shareholders held on June 10, 2015 amendments to our 2014 Share Incentive Plan (1) to increase the number of shares reserved for issuance under the plan by 610,027 shares, representing 2% of our outstanding ordinary shares as of December 31, 2014, and (2) to increase from 2% to 4% the percentage of our outstanding share capital as of each year end by which the pool of ordinary shares may increase on an annual basis under the evergreen provision of the plan.

Unless otherwise indicated, this prospectus assumes (1) no exercise of the underwriters' option to purchase up to 735,000 additional ordinary shares from the selling shareholders and (2) no exercise of outstanding options or vesting of RSUs after March 31, 2015.

**Table of Contents****Summary Consolidated Financial Data**

The following tables set forth our summary consolidated financial data. You should read the following summary consolidated financial and other data in conjunction with Selected Consolidated Financial Data, Management's Discussion and Analysis of Financial Condition and Results of Operations and our consolidated financial statements and related notes included elsewhere in this prospectus. Historical results are not necessarily indicative of the results that may be expected in the future. Our financial statements have been prepared in accordance with U.S. Generally Accepted Accounting Principles, or U.S. GAAP.

The summary consolidated statements of operations data for each of the years in the three-year period ended December 31, 2014 is derived from our audited consolidated financial statements appearing elsewhere in this prospectus. The summary consolidated statement of operations data for the three months ended March 31, 2014 and 2015 and the summary balance sheet data as of March 31, 2015 are derived from our unaudited interim consolidated financial statements presented elsewhere in this prospectus. In the opinion of management, these unaudited interim consolidated financial statements include all adjustments, consisting of normal recurring adjustments, necessary for a fair statement of our financial position and operating results for these periods. Results for interim periods are not necessarily indicative of the results that may be expected for the entire year.

	Year ended December 31,			Three months ended March 31,	
	2012	2013	2014	2014	2015
	(in thousands, except share and per share amounts)				
<b>Consolidated Statements of Operations:</b>					
Revenues:					
License	\$ 27,029	\$ 38,907	\$ 61,320	\$ 9,120	\$ 19,978
Maintenance and professional services	20,179	27,250	41,679	8,275	12,937
<b>Total revenues</b>	<b>47,208</b>	<b>66,157</b>	<b>102,999</b>	<b>17,395</b>	<b>32,915</b>
Cost of revenues:					
License	1,002	1,216	2,654	628	550
Maintenance and professional services	5,922	7,860	12,053	2,425	3,707
<b>Total cost of revenues(1)</b>	<b>6,924</b>	<b>9,076</b>	<b>14,707</b>	<b>3,053</b>	<b>4,257</b>
<b>Gross profit</b>	<b>40,284</b>	<b>57,081</b>	<b>88,292</b>	<b>14,342</b>	<b>28,658</b>
Operating expenses:					
Research and development(1)	7,273	10,404	14,400	3,237	4,117
Sales and marketing(1)	22,081	32,840	44,943	9,433	13,460
General and administrative(1)	3,297	4,758	8,495	1,481	3,578
<b>Total operating expenses</b>	<b>32,651</b>	<b>48,002</b>	<b>67,838</b>	<b>14,151</b>	<b>21,155</b>

Edgar Filing: CyberArk Software Ltd. - Form 424B4

Operating income	7,633	9,079	20,454	191	7,503
Financial income (expenses), net	4	(1,124)	(5,988)	(1,356)	(1,631)
Income (loss) before taxes on income	7,637	7,955	14,466	(1,165)	5,872
Tax benefit (taxes on income)	225	(1,320)	(4,512)	(83)	(1,706)
Net income (loss)	\$ 7,862	\$ 6,635	\$ 9,954	\$ (1,248)	\$ 4,166
Basic net income (loss) per ordinary share(2)	\$ 0.51	\$ 0.25	\$ 0.46	\$ (0.35)	\$ 0.14
Diluted net income (loss) per ordinary share(2)	\$ 0.31	\$ 0.14	\$ 0.34	\$ (0.35)	\$ 0.12
Weighted average number of ordinary shares used in computing basic net income (loss) per ordinary share(2)	6,592,997	6,900,433	13,335,059	7,073,239	30,563,888
Weighted average number of ordinary shares used in computing diluted net income (loss) per ordinary share(2)	25,245,790	10,765,914	29,704,730	7,073,239	34,786,581

**Table of Contents**

	<b>As of March 31, 2015</b>				
	<b>Actual</b>	<b>As Adjusted(4)</b>			
	<b>(in thousands)</b>				
<b>Consolidated Balance Sheet Data:</b>					
Cash, cash equivalents and short-term bank deposits	\$ 191,668	\$243,673			
Deferred revenue, current and long-term	41,331	41,331			
Working capital(3)	168,856	220,984			
Total assets	222,060	274,436			
Total shareholders' equity	160,440	212,816			
	<b>Year ended December 31,</b>			<b>Three months ended March 31,</b>	
	<b>2012</b>	<b>2013</b>	<b>2014</b>	<b>2014</b>	<b>2015</b>
	<b>(in thousands)</b>				
<b>Supplemental Financial Data:</b>					
Non-GAAP operating income(5)	\$ 7,917	\$ 9,482	\$ 22,027	\$ 347	\$ 9,049
Non-GAAP net income(5)	8,322	8,484	15,836	304	5,712
Net cash provided by operating activities	13,657	20,159	23,840	8,898	