Mimecast Ltd
Form 10-K
May 29, 2018

UNITED STATES

SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-K

(Mark One)

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
For the fiscal year ended March 31, 2018

OR

TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 FOR THE TRANSITION PERIOD FROM TO .
Commission File Number 001-37637

MIMECAST LIMITED

(Exact name of Registrant as specified in its Charter)

| | |
|---|---|
| Bailiwick of Jersey<br>(State or other jurisdiction of<br><br>incorporation or organization) | Not Applicable<br><br>(I.R.S. Employer<br>Identification No.) |
| CityPoint, One Ropemaker Street, Moorgate<br><br>London EC2Y 9AW | |
| United Kingdom<br>(Address of principal executive offices) | EC2Y 9AW<br>(Zip Code) |

Registrant’s telephone number, including area code: (781) 996-5340

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

| | |
|---|---|
| Ordinary Shares, nominal value $0.012 per share | The Nasdaq Stock Market LLC |
| (Title of each class) | (Name of each exchange on which registered) |

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

None

(Title of class)

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

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Act. YES NO

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 NO

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). YES NO

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§229.405) is not contained herein, and will not be contained, to the best of registrant’s knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K.

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

| | | |
|---|---|---|
| Large accelerated filer | | Accelerated filer |
| Non-accelerated filer | (Do not check if a small reporting company) | Small reporting company |
| | | Emerging growth company |

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). YES NO

The aggregate market value of the voting and non-voting common equity held by non-affiliates of the registrant, based on the closing price of our ordinary shares on the NASDAQ Global Select Market on September 29, 2017, the last business day of the registrant's second fiscal quarter, was $954,261,949. This calculation does not reflect a determination that certain persons or entities are affiliates of the registrant for any other purpose.

The number of registrant's ordinary shares outstanding as of May 15, 2018 was 58,976,977.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's Definitive Proxy Statement relating to the 2018 Annual General Meeting of Shareholders, scheduled to be held on October 4, 2018, are incorporated by reference into Part III of this Report. The Definitive Proxy Statement will be filed with the Securities and Exchange Commission within 120 days of the registrant's fiscal year ended March 31, 2018.

Table of Contents

SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K contains forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. All statements contained in this Annual Report on Form 10-K other than statements of historical fact, including statements regarding our future results of operations and financial position, our business strategy and plans, and our objectives for future operations, are forward-looking statements. These statements involve known and unknown risks, uncertainties and other important factors that may cause our actual results and performance to be materially different from any future results or performance expressed or implied by the forward-looking statements. The words “believe,” “may,” “will,” “estimate,” “continue,” “anticipate,” “intend,” “expect,” “predict,” “potential,” “should,” “contemplate,” “would,” “project,” “seek,” “target,” “might,” “plan,” “strategy,” and similar expressions or variations not statements of historical fact are intended to identify forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements set forth in this this Annual Report on Form 10-K include, but are not limited to, the following:

- our expectations regarding our revenue, expenses and other results of operations;
- our plans to invest in sales and marketing efforts, increase the size of our sales and marketing team, and expand our channel partnerships;
- our ability to attract new customers and retain existing customers;
- our plans to continue to invest in the research and development of technology for both existing and new products, and increase the size of our research and development team;
- the growth rates of the markets in which we compete;
- our liquidity and working capital requirements;
- our anticipated strategies for growth;
- our ability to anticipate market needs and develop new and enhanced solutions to meet those needs;
- our ability to compete in our industry and innovation by our competitors;
- our ability to adequately protect our intellectual property;
- our ability to respond to evolving regulatory requirements regarding data protection and privacy, including the European Union’s General Data Protection Regulation; and
- our plans to pursue strategic acquisitions.

We caution you that the foregoing list may not contain all of the forward-looking statements made in this Annual Report on Form 10-K.

You should not rely upon forward-looking statements as predictions of future events. We have based the forward-looking statements contained in this Annual Report on Form 10-K primarily on our current expectations and projections about future events and trends that we believe may affect our business, financial condition, operating results and prospects. The outcome of the events described in these forward-looking statements is subject to risks, uncertainties and other factors described in Part I, Item 1A, “Risk Factors” in this Annual Report on Form 10-K. Moreover, we operate in a very competitive and rapidly changing environment. New risks and uncertainties emerge from time to time, and it is not possible for us to predict all risks and uncertainties that could have an impact on the forward-looking statements contained in this Annual Report on Form 10-K. We cannot assure you that the results, events and circumstances reflected in the forward-looking statements will be achieved or occur, and actual results, events or circumstances could differ materially from those described in the forward-looking statements.

The forward-looking statements made in this Annual Report on Form 10-K relate only to events as of the date on which the statements are made. We undertake no obligation to update any forward-looking statements made in this Annual Report on Form 10-K to reflect events or circumstances after the date of this Annual Report on Form 10-K or to reflect new information or the occurrence of unanticipated events, except as required by law. We may not actually achieve the plans, intentions, or expectations disclosed in our forward-looking statements and you should not place undue reliance on our forward-looking statements. Our forward-looking statements do not reflect the potential impact

of any future acquisitions, mergers, dispositions, joint ventures, or investments we may make.

As used in this Annual Report on Form 10-K, the terms “Mimecast,” “Company,” “Registrant,” “we,” “us,” and “our” mean Mimecast Limited and its subsidiaries, unless the context indicates otherwise.

PART I

Item 1. Business.

We are a leading global provider of cloud cyber resilience solutions for corporate data and email. Email is the number-one threat vector. Our fully-integrated, pure cloud services protect customers across the globe from incidents that typically start with email, including advanced cyberattacks, data loss, downtime, and human error. We mitigate the significant business disruption caused by email failure and downtime. Our cloud archive secures, stores and manages data, while addressing compliance, regulatory and e-discovery requirements, and improving employee productivity.

Email is a critical tool for organizations of all sizes. Protecting and managing email has become more complicated due to expanding security and compliance requirements and the rapid increase in both the volume and the importance of the information transmitted via email. Organizations are increasingly at risk from security breaches of sensitive data as sophisticated email-based attacks or data leaks have become far more common than in the past. Additionally, organizations are not just using email for communication. Email archives are used as an active repository of vital corporate information needed to meet compliance and regulatory requirements and ensure employee productivity. As a result, email represents one of the highest concentrations of business risk that organizations face.

Traditional approaches to addressing these risks leave customers managing disparate point products from multiple vendors that are often difficult to use, costly to manage, difficult to scale, can fail to fully address advanced threats, and limit the use of corporate information to enhance productivity. The resulting infrastructure complexity caused by disparate products and legacy architectures also makes it difficult to move more IT workloads to the cloud, which continues to be an increasing priority of organizations of all sizes.

We developed our proprietary cloud architecture to offer customers a comprehensive cyber resilience strategy for email that spans security, continuity, archiving and end-user empowerment. These capabilities are delivered from an easy-to-use single platform. Providing a fully-integrated service also simplifies ongoing management and service deployment. Our customers can then decommission the often costly and complex point products and on-premises technology they have traditionally used to address these risks. We also make it easier for customers to move more of their IT workloads to the cloud.

We serve approximately 30,400 customers and protect millions of their employees around the world. Our service scales effectively to meet the needs of customers of all sizes. We sell our services through direct sales efforts and through our channel partners. Our sales model is designed to meet the needs of small and mid-market organizations and large enterprises across a wide range of industries and in over 130 countries. We have approximately 1,200 employees in twelve offices in the United States, the United Kingdom, South Africa, Australia, Dubai, UAE, the Netherlands and Germany. For the fiscal years ended March 31, 2018, 2017 and 2016, our revenue was $261.9 million, $186.6 million and $141.8 million, respectively.

Industry Background

Email is a critical tool for organizations of all sizes. Email also captures a comprehensive history of corporate activity, knowledge and data vital for day-to-day business operations and employee productivity. Consequently, email needs protection and the technology needed to do this has extended well beyond the mailbox itself to include additional security, continuity and archiving services, all of which have typically been offered by separate vendors with different approaches.

While our industry is rapidly evolving, we believe the following reflect the key themes and compelling trends that are important to understanding our industry:

- Email is critical to all organizations;
- Many critical IT systems rely on email to operate effectively;
- Email is a primary security target for advanced cyberattacks;
- The amount of critical and sensitive data in email archives is growing rapidly;
- Data protection, cybersecurity and data privacy are key compliance and regulatory concerns for all organizations;
- Email downtime is disruptive to employee productivity;
- IT workloads, including business productivity tools, are moving to the cloud;
- Business email mailboxes are moving to the cloud, but this creates new risks to mitigate;

- Traditional email security, continuity and archiving alternatives can be inadequate and may not address increasing customer requirements and protect against next generation security threats;
- Point products are inflexible and only address part of the problem; and
- Traditional on-premises or hosted architectures have performance limitations and are expensive.

The limitations of traditional security and archiving technologies mean customers need to rethink their approach to protecting email and corporate information. We believe organizations are ultimately looking to implement a multi-layered cyber security and resilience strategy that delivers protection of users, data and operations from the risks arising from technological failure, human error and malicious intent. The risks also increase with organizations migrating to Microsoft Office 365®, as it is a complex email solution that is a high value and high-profile target. Organizations also need robust continuity options to solve for unpredictable events that cause an outage to email and result in disruption to business. A multi-layered cyber security and resilience approach is needed in order to address the diverse threats and diverse data classifications within a single data environment.

Meeting this growing customer demand requires an email and data security cloud service that meets the following requirements:

- Integrated Offering. By bringing multiple requirements into a cyber resilience solution for data and email platform, our next-generation email service helps organizations reduce the complexity and cost of managing point technologies from disparate vendors and brings additional benefits from new capabilities made possible due to the platform, and cloud delivery.
- Strong Technology. As organizations substitute specialized products provided by different vendors, it is imperative that the individual products are as good, or better, than those being replaced. Organizations are not willing to compromise on performance or security at a product level.
- Native Cloud. As organizations shift workloads to the cloud and move away from retaining on-premises or single tenant hosted cloud infrastructure, today's email security and information management technology must be natively cloud-based, thereby eliminating the need for local software and hardware, virtual machines and device hosting.
- Built-for-Scale. As email traffic and data storage continues to increase dramatically, the risk of threats escalates and the need for real-time, on-demand email access becomes more prominent, organizations cannot compromise on email performance and availability. The ideal solution must be easily scalable to match customer demand and be able to handle large volumes.
- Easy-to-Deploy and Manage. A cloud platform should simplify the process of service updates, new product deployments and on-boarding. System improvements should also be handled centrally, reducing this burden for the customers' own IT team. A fully-integrated service also means it should be managed from a single administration console.
- Adaptable to Customer Needs. With the rapidly shifting threat landscape and other IT requirements, customers' email needs are continuously evolving. It is important that email and information management solutions adapt quickly to help organizations keep pace with changing risks and enhance productivity.
- Lower Total Cost of Ownership. The most-effective approach for corporate email security, continuity, archiving and data management is to solve the current problems of integration, performance and scalability while simplifying the IT email infrastructure and reducing the initial capital outlay, recurring maintenance costs and growing storage costs that many companies face as their volumes scale.

Our Market Opportunity

The United States Census Bureau estimates there are approximately 5.8 million organizations employing 121.1 million employees in the United States. Among them, there are over 610,000 small and mid-size organizations, which are defined as those organizations employing 20 to 4,999 employees that together have approximately 59 million employees. Based on a recent Gartner report, worldwide combined spending will total approximately $3.0 billion for the secure email gateway and data loss prevention markets. IDC Research estimates the markets for backup and recovery software, and e-discovery software will grow to $11.8 billion. Based on these reports, the combined markets catering to enterprise information and email security, continuity and archiving are estimated to be $14.8 billion in 2020. We believe there is a considerable need for a comprehensive integrated cloud solution that can address the needs of customers in these markets.

We believe our immediate opportunity is to replace incumbent email security, continuity and archiving vendors. As we extend our products into adjacent areas, we anticipate this will open up additional opportunities to take further market share in a wider range of enterprise security and data management markets. We also expect to benefit from the growing popularity of cloud email services, specifically Microsoft Office 365® and Google, and the customer need for complementary security, archiving, back-up and continuity services.

Our Solution

Our integrated suite of cloud services for security, continuity and archiving is designed to offer true cyber resilience for email and deliver comprehensive email risk management beyond the primary mail server. We protect customers from the growing threat from email and to the corporate data it contains from malware, spam, data leaks and advanced threats such as impersonation attacks. Our continuity services ensure email and corporate information remain available in the event of a primary system failure or scheduled maintenance downtime. We also help organizations securely and cost effectively archive their growing email and file repositories to support employee productivity, compliance and e-discovery.

Our customers benefit from:

- Comprehensive Email and Data Risk Management in a Single, Unified Cloud Service. Our services integrate a range of technologies into a comprehensive service that would otherwise require an array of individual devices or services from multiple vendors. We enable customers to decommission these technologies, reduce the cost and complexity of their infrastructure, redeploy IT resources, and improve the security and risk management of their corporate email environment.

- Best-of-Breed Security, Continuity and Archiving Services. We believe our customers should not have to compromise on the quality of their email security, continuity or archiving services in order to benefit from integration. Our strategy is to develop best-of-breed capabilities within our integrated service to compete successfully with industry-leading point products in three critical areas:
- Email and Data Security: We protect customers from a comprehensive range of email and data related threats that include, but are not limited to, spam, viruses, impersonation attacks, phishing and spear phishing, identity theft, advanced persistent threats, malicious attachments, known and unknown malware, outbound spam outbreaks and malicious inbound URLs, extortion and fraud. We combine our proprietary cloud-based scanning, detection and real-time intelligence gathering technologies with third-party threat data and malware libraries to deliver comprehensive and overlapping protection reflective of a best-of-breed security service.
- Email Service Continuity: Our continuity service enables customers to send, receive and view emails and calendars during email gateway failures or planned maintenance downtime, without the need to build or host their own replicated email environment. Our service has immediate fail-over and fail-back capabilities, and is fully-integrated into Microsoft Outlook®. Employees can continue to access their email and data using their preferred mobile, tablet or desktop device, or via our web-based portal, so there is limited interruption to normal operations.
- Data Archiving: We enable organizations to archive rapidly growing volumes of email and associated data safely and centrally in the cloud to support their need to archive data cost effectively to meet long-term storage, compliance, governance, risk mitigation and regulatory obligations. We also provide powerful search tools that can increase employee productivity, and enable them to utilize their archive as a live file store. Key features of our service include unlimited and perpetual legal hold, discovery and early legal case assessment, onsite and cloud-linked retention management, administrator and employee-led retention controls, onsite and metadata synchronization and record destruction policies and services.
- Web Scale Performance for Organizations of All Sizes. Our cloud service is built to address the most demanding scale, performance and availability requirements of large enterprises but delivers this as a subscription-based cloud service that puts these capabilities within the reach of small and mid-market organizations too. Our data centers process approximately 379 million emails per day, and store over 260 billion emails and approximately 40 petabytes of customer data. We achieve demanding continuity service commitments with data centers that are replicated in each of our primary geographies and operate in active-active mode enabling fast failover and fail-back as required.
- Easy to Deploy and Manage. Our service is designed to be easier to deploy than alternative technologies. Customers simply route their email traffic through our cloud and can be up and running in a matter of days and sometimes less. We then enable our customers to add or delete new services and employees, and manage all security and other policies centrally via a single web-based administration console that significantly simplifies the ongoing management of their email and data environment.
- Highly Agile and Adaptable Service. We are continually improving our cloud architecture and services. Our common code base and multi-tenant cloud architecture enables us to perform maintenance updates and add new features or products without interruption to our customers. Continuous service development and multi-tenant rapid deployment also allows us to keep pace with emerging threats to protect and respond quickly to changing customer needs.
- An Easier Move of Additional Critical Workloads to the Cloud. For those customers that want to put more workloads into the cloud, our technology facilitates the migration of email in particular by removing the complexity that has stalled many customers to date. Our interoperability with cloud-based email servers, such as Microsoft Office 365®, makes this easier to achieve and helps to mitigate remaining concerns about the single-vendor security, data integrity and continuity risk of such a move. Our data ingestion offering also allow customers to bring legacy data into their new cloud archive to ensure it is a complete record of current and historic data.
- Compelling Return on Investment. Our unified, cloud-based service enables our customers to decommission a range of legacy and disparate technologies that support their email server and recover these costs. We utilize hardware efficiently, and share a single instance of the operating software as well as storage and processing hardware securely across the whole customer base within each data center, allowing us to deliver cloud-scale economic and performance benefits to our customers. Customers also benefit from the continuous improvement of our service without the need to pay for service packs or updates. Our service bundles and subscription-based pricing also enable

customers to pay per employee and select their desired services making costs easy to predict and affordable.

5

Our Growth Strategy

We will continue to invest in cloud security and risk management services. As more organizations move IT workloads such as email to the cloud, we believe we are well positioned to continue capitalizing on this growing opportunity globally.

Our growth strategy is focused on the following:

- Grow Revenue From Our Existing Customer Base. We serve approximately 30,400 customers of all sizes. We provide a high level of service that results in our customers staying with us year over year, which has resulted in a revenue retention rate of 110% and 111% for the fiscal years ended March 31, 2018 and 2017, respectively. This large and loyal customer base provides us with the opportunity to sell additional services and add more employees to their subscriptions. We believe we have significant upsell potential in our existing customer base with current and new services. We intend to continue proactively broadening our reach within our existing customer base by selling additional services.
- Acquire New Customers. We have built our global cloud architecture to offer best-of-breed capabilities and to be highly scalable and affordable for organizations of any size, ranging from small and mid-market customers to the largest global enterprises. Moreover, we offer our security, continuity and archiving email services as bundles and in a modular fashion, enabling us to win new customers by addressing a variety of initial needs and use cases that we expand over time as we cross sell other offerings. We will continue to invest in a direct sales force combined with a focused channel strategy designed to serve the various requirements of small, mid-market and large enterprises and to bring new customers onto our cloud architecture.
- Actively Invest in Our Channel Partner Network. The majority of our sales are through a reseller channel designed specifically to meet the requirements of each of our target customer segments. In the large enterprise market, we are building on existing relationships with leading systems integrators. In small and mid-market organizations, we are extending our network of leading IT resellers. We expect to expand our channel strategy over time to incorporate additional security or cloud specialists, as well as resellers focusing on supporting customers with the transition to Microsoft Office 365®. We intend to further invest in our network of channel partners to further extend our global sales, service and support capabilities.
- Develop Our Technology and Release New Services. We regularly update and improve our software and architecture and seamlessly deploy these updates to our customers. We will continue to build on our current capabilities and exploit additional opportunities in adjacent areas to those we serve today. This will extend the value our customers can gain from our architecture and enable them to consolidate additional email and data services to our integrated cloud service working seamlessly with Microsoft Exchange®, Microsoft Office 365® and G-Suite from Google®.
- Continue to Expand Our Geographic Presence. We were founded outside the United States and, consequently, 51% of our sales in fiscal years 2018 and 2017 were derived from non-U.S. locations. We view the United States as our most significant growth market. Since founding our U.S. business in 2008, we have established a successful direct sales channel and service infrastructure to exploit this opportunity. In fiscal year 2018, we launched our German operation, which will become fully operational in fiscal year 2019. We plan to investigate additional international expansion from our regional bases in the United States (for North America), the United Kingdom and Germany (for Europe), South Africa (for Africa and the Middle East), and Australia (for Asia-Pacific).
- Target Organizations Moving Workloads to the Cloud. Given the compelling cost benefits and improved agility of cloud-based solutions, organizations are increasingly moving critical workloads to the cloud. As these IT workloads move to the cloud, we believe we are well-positioned to take advantage of growth opportunities that exist from augmenting services, including Microsoft Office 365® and G-Suite from Google®.
- Growth Through Acquisitions. We believe there is a significant opportunity to grow our business by acquiring complementary products, technologies and businesses. We look for products and technologies that will enable us to expand our offerings to our existing customer base and attract new customers that we were not able to service with our existing offerings. We also believe that acquisitions give us access to potential employees with industry

experience that may not otherwise be available to us.

Our Technology

We have developed a native cloud architecture, including our own proprietary software as a service, or SaaS, operating system, Mime | OS™, and customer-facing services, to address the specific risks and functional limitations of business email and data. Our innovative cloud-based approach requires no on-premises or hosted appliances. We believe we are one of only a few cloud service providers that have fully committed to native cloud development.

We have a proven record of performing successfully at considerable scale and addressing rapidly growing customer demands. We process approximately 379 million emails per day and manage over 260 billion emails in total with our service. We archive approximately 40 petabytes of customer data and add more than 65.9 terabytes of customer data per month.

We are able to provision customer email and onboard massive amounts of email data from legacy archives rapidly and efficiently. This drives customer adoption and makes the cloud transition easier than our customers typically expect. Once a customer is live on our service, adding new products to their subscription only requires activation from within their single administration console.

Our Proprietary Native Cloud Architecture— Mime | OS™

We developed a proprietary operating system called Mime | OS™ for native cloud services. Mime | OS™ enables secure multi-tenancy and takes advantage of the cost and performance benefits of using industry-standard hardware and resource sharing specifically for the secure management of email and data. This enables us to provision efficiently and securely across our customer base, minimizing the impact of spare or over-provisioned processing and storage capacity, reducing the cost of providing our services.

Mime | OS™ comprises 20+ microservices that control the hardware, and the storage, indexing, processing, services, administrator and user interface layers of our cloud environment. It has been specifically designed to enable us to scale our storage, processing and services to meet large enterprise-level email and data demands, while retaining the cost and performance benefits of a native cloud environment.

Mime | OS™ also streamlines our customer application development and enables strong integration across our services. All of our customer applications or services use Mime | OS™ to interact with our data stores and processing technology, as well as interoperate effectively with each other.

Continuous Development Methodology and Multi-Tenancy Advantage

As we enhance and expand our technology, we can update services centrally with little or no intervention required by the customer, as each customer shares the same core operating and application software. Improvements, upgrades, new products or patches are applied once and are available immediately across our whole service to customers. It means we have only one up-to-date version of our service to maintain and support as well as a common data store for all customers that simplifies management, support and product development.

Our services already process and manage large volumes of customer data and this is growing daily. Our commitment to continual improvement in Mime | OS™, our customer applications and hardware infrastructure mean we are constantly strengthening the performance of our service as we scale. These improvements include faster archive search times and data ingestion, greater storage density, improved processing and extended security coverage. Each week, we roll out updates and enhancements centrally that benefit our customers without the need for additional infrastructure investment on their part. Additionally, when new threats emerge, we act once by making changes to our service and all customers benefit immediately. We can also identify and act on threats to one customer and quickly prevent them from impacting others by changing our core system.

How Our Services Work

Mimecast Advanced Security

We protect inbound and outbound email from malware, spam, advanced persistent threats, email DoS and DDoS, data leaks and other security threats.

Inbound email is directed through Mimecast Email Security, which performs comprehensive security checks before the email is delivered to the customer's email infrastructure. This prevents unwanted email from reaching the customer in the first place and cluttering their infrastructure unlike on-premises services from competitors. Each day, we monitor approximately 820 million messages and deliver, on average, less than 50% of those messages to the customer.

Outbound email sent from the customer also passes through our service and is checked before being sent on to prevent it from presenting a security threat to the recipient. Outbound email can also be encrypted, and scanned by our comprehensive content controls to prevent confidential documents or data leaving the business. Data leak prevention is a key consideration for all organizations.

Mimecast Business Continuity

Email is a 24x7 tool and, traditionally, customers who want to ensure their email does not experience downtime as a result of an inevitable outage or maintenance have had to replicate their own infrastructure in a second location, doubling their email-related costs. The cost and management burden of doing this is prohibitive for many, particularly small or mid-market organizations.

We are a cost-effective alternative as there is no need for additional infrastructure. As all customer outbound and inbound email is directed to our servers, if a customer's primary email service fails, our Mimecast Mailbox Continuity service takes over the delivery and sending of email in real time or at the request of the administrator, offering immediate fail-over and fail-back. When the primary service is re-established, the customer is reassured that there has been no loss of data and that the archive is maintained. For employees, the process is virtually invisible—they continue to work as before in their Microsoft Outlook® desktop email client, their Mimecast mobile app or their Mac® Desktop App.

Mimecast Enterprise Information Archiving

Email, and the data it contains, needs to be safely archived to meet growing compliance, regulatory and legal obligations. Also, employees are increasingly using their email archive as their primary information store so this is further reason to ensure it is protected and archived effectively.

As email, file attachments, and associated critical metadata that identifies activity is sent or received, it can be saved in a secure, tamper-proof archive in the single Mimecast cloud automatically and indefinitely. Our employee mobile and desktop search tools and administration console, then allow for detailed investigation of the archive. We also enable customers with legacy archive data to put this into their single Mimecast archive, which improves adherence to data compliance obligations and gives employees access to a complete historical view of their archive.

Our Mimecast Enterprise Information Archiving service offers secure lifetime storage of email, files and instant messaging conversations paid for on a per-employee basis and not on a data usage basis. By switching to the Mimecast Enterprise Information Archiving Service, expensive and ineffective onsite archives can be decommissioned, reducing the data load on the primary email service too. Our search tools make it easy for legal staff and employees themselves to quickly find data without the need to turn to the IT team. Finally, our archive can also include legacy data that would otherwise be held in additional storage. This can be ingested over-the-wire or via physical drives sent encrypted from the customer to us.

Our Global Data Center Network

We have built networks in twelve data centers in six locations around the world to deliver our services. This gives customers geographic and jurisdictional control over data location, which enables them to address data privacy concerns. Each region operates two identical data centers that function in active-active mode in different locations, and have N+1 set-ups to meet our continuity of service commitments. Because of this redundancy, we are able to switch operations from one data center to another to maintain our customers' email and data services. We have developed a modular approach to provisioning a new data center and can transition among data centers as needed in existing or new geographies. Our twelve co-located data centers are replicated and operate in active-active mode to allow for continuity of service in the event of downtime or maintenance.

Our Services

Our email security, continuity and archiving services protect customer data, providing organizations comprehensive email risk management in a single, cloud-based, fully-integrated service, which is licensed on a subscription basis.

- The Mimecast Email Security service protects against the delivery of malware, malicious URLs, spam, spear-phishing attacks, including business email compromise, and other emerging attacks, while also preventing data leaks and other internal threats.
- The Mimecast Mailbox Continuity service ensures employees can continue using email during unexpected and planned outages such as system maintenance, whether their email is managed in the cloud or on-premises.
- Mimecast Enterprise Information Archiving unifies email, data to support e-discovery and forensic analysis, and gives employees fast access to their personal archive via PC, Mac® and mobile apps.

Mimecast Advanced Security

Email security provides a critical defense against hackers seeking to capture and exploit valuable organizational information and disrupt business operations. Our Mimecast Email Security services provide comprehensive email security. They block spam, malware, malicious URLs, spear-phishing, and defined content from entering or exiting the organization. Further, these services provide administrators granular security and content policy control for inbound, outbound, and internal email traffic to prevent threats, including data leaks. Integration into Microsoft Outlook® and via mobile apps provides employees the freedom to be self-sufficient and to manage their quarantines, personal blacklists, and many other aspects of their email security and management.

Customers can benefit from the following Mimecast security services:

- Targeted Threat Protection: Highly sophisticated targeted attacks, including spear-phishing, are using email to successfully infiltrate organizations, exploit users and steal valuable intellectual property, customer data and money.
- URL Protect addresses the threat from emails containing malicious links. It automatically checks hyperlinks each time they are clicked, preventing employees from visiting malicious websites regardless of what email client or device they are using. It also includes innovative user awareness capabilities so IT teams can raise the security awareness of employees as part of their daily email activities. Once enabled, a percentage of links in emails clicked by an employee will open an informational screen. This will provide them with more information about the email and destination, encouraging them to consider whether the email is coming from a reliable source and if the page is safe. If they choose to continue, the choice is logged and URL Protect scans the link and blocks access if the destination is deemed unsafe. IT administrators can adjust the frequency of these awareness prompts to ensure employee caution is maintained. Repeat offenders that regularly click bad links can automatically receive more frequent prompts until their behavior changes. The IT team can track employee behavior from the Mimecast administration console and target additional security training as required.
- Attachment Protect reduces the threat from weaponized or malware-laden attachments used in spear-phishing and other advanced attacks. It includes pre-emptive sandboxing to automatically security check email attachments before they are delivered to employees. Attachments are opened in a virtual environment, or sandbox, isolated from the email system, security checked and passed on to the employee only if no threat is detected. It also includes the option of an innovative safe file conversion capability that automatically converts attachments into a safe file format, neutralizing any chance of malware as it does so. The attachment is delivered to the employee in read-only format without any sandbox analysis delay. As most attachments are read rather than edited, this is often sufficient for many users. Should the employee need to edit the attachment, they can request it and from there it is sandboxed on-demand and delivered in the original file format.
- Impersonation Protect gives instant and comprehensive protection from malware-less social engineering attacks, often called CEO fraud, whaling, impersonation, or business email compromise. These attacks are designed to trick users, most particularly key employees such as those who are on an organization’s finance team, into making wire transfers or other financial transactions to cybercriminals by pretending to be the CEO or CFO via spoofed email. Some impersonation attacks also target those responsible for managing sensitive employee data, such as payroll information, which could be used for identity theft. Impersonation Protect detects and prevents these types of attacks by identifying combinations of key indicators in an email to determine if the content is likely to be suspicious, even in the absence of a URL or attachment. Impersonation Protect blocks or flags suspicious email by using advanced scanning techniques to identify elements commonly used by criminals, including employee, domain, or reply-to names, and other keywords such as ‘wire transfer,’ ‘tax form’ or ‘urgent.’
- Internal Email Protect, or IEP, is the industry’s first threat management capability for internally generated email delivered by a purely cloud-based security service. IEP allows customers to monitor, detect and remediate security threats that originate from within their internal email systems. This capability provides for the scanning of attachments, URLs, and content in internally generated email. In addition, IEP includes the ability to automatically remediate infected email from a user’s inbox.

- Secure Messaging: Email containing sensitive or confidential information requires appropriate security and control to prevent inadvertent or deliberate data leaks and to protect the information while in transit. Mimecast Secure Messaging is a secure and private channel to share sensitive information with external contacts via email without the need for additional client or desktop software. Sensitive information is kept within the Mimecast cloud service, strengthening information security, data governance and compliance, without the added IT overhead and complexity of traditional email secure messaging or encryption solutions.

- Large File Send: Employees can create security and compliance risks when they turn to file sharing services to overcome email size limits imposed by their email infrastructure. Mimecast Large File Send enables PC and Mac® users to send and receive large files directly from Microsoft Outlook® or a native Mac® app. It protects attachments in line with security and content policies by using encryption, optional access key and custom expiration dates; supports audit, e-discovery and compliance by archiving all files and notifications according to email retention policies; and protects email system performance from the burden of large file traffic.
- Data Leak Prevention: Organizations can prevent the inadvertent or malicious loss of sensitive corporate data with advanced data leak prevention and content controls. Policies using keywords, pattern matching, file hashes and dictionaries actively scan all email communications including file attachments to stop data leakage and support compliance. Suspect emails can be blocked, quarantined for review by administrators or sent securely.

Mimecast Business Continuity

Email continuity protects email and data against the threat of downtime as a result of system failure, natural disasters, planned maintenance, system upgrades and migrations. Mimecast Mailbox Continuity services significantly reduce the cost and complexity of mitigating these risks and provides uninterrupted access to live and historic email and calendar information. During an outage our service provides real-time inbound, outbound and internal email delivery. The continuity service can be activated and deactivated directly and instantly from the Mimecast console by administrators for the complete organization or for specific groups affected by limited outages. All outage events are fully logged and we also support email top-up services for customers who have to recover their Microsoft Exchange® environments from backups. The continuity service is capable of reliably and securely supporting customers during short or long-term continuity events. Integration with Microsoft Outlook®, a native app for Mac® users and a full suite of mobile apps means employees have seamless access to their email in the event of a disruption or outage.

Mimecast Enterprise Information Archiving

Our cloud archive consolidates into one store all inbound, outbound and internal email, files and instant messaging in a perpetual, indexed and secure archive. Using our Mimecast Enterprise Information Archiving service, customers can also incorporate legacy data from additional archives into the same searchable store.

All data is encrypted and preserved within a Write Once Read Many (WORM) state. Proprietary indexing and retrieval solutions allow customers to search individual mailboxes or the entire corporate archive in seconds. Our mobile, tablet, desktop and web applications ensure that employees can search and make the best use of their entire corporate archive in a fast, reliable and informative way. Intensive logging services cover the use of the archive, and roles and permissions govern what employees can see in the archive based on their role. Our purpose-built ingestion and export services support rapid high-volume extraction, scrubbing and loading of significant quantities of data. Our archive solution retains metadata that arises from gateway and continuity operations and we preserve both received and altered variants of emails that pass through our secure email gateway. Retention options for customers range from individual retentions, to data retained for an entire customer on a perpetual basis.

Customers can also purchase the following additional services as part of our Mimecast Enterprise Information Archiving offering:

- Recoverability: Email continues to be the preferred business communication tool and de facto data repository. It holds vast amounts of critical and sensitive information. Protecting this data against loss or corruption and managing spiraling inboxes is imperative. Mimecast Sync & Recover for Exchange® and Office 365® offers three key capabilities that expand on the built-in tools provided by Mimecast Archiving alone including Sync & Recover, Granular Retention Management and Mailbox Storage (Stubbing) Management. Sync & Recover delivers rapid and granular recovery of mailboxes, calendar items and contacts lost through inadvertent or malicious deletion or corruption.

- Archive Power Tools: This is a series of advanced archiving tools including:
- Mimecast Storage Management for Exchange: This enables active mailbox size management, so administrators can optimize email system performance, control costs and support archive policy enforcement.
- Mailbox and Folder Tools for Exchange: In an email continuity event or when searching for archived content, access to folder structures and shared mailbox content is key to productivity. This tool makes it easy to replicate individual and shared mailbox folders.
- Granular Retention Management: Managing email retention policies can be complex and time-consuming, because different business groups and individuals have requirements that vary how long email should, or is required to be retained. Mimecast Granular Retention Management enables IT teams to centrally apply policies to manage the retention of email content and related metadata.

Service Bundles

Many of our customers take advantage of the ability to combine our services and capabilities into a unified service managed from a single administration console. Most customers purchase the bundles from the outset, but some prefer to start with specific packages, then upgrade to additional products over time.

Our service range continues to respond to the changing threat landscape and reflect customers' requests for combinations of services across advanced security, continuity and archiving. We transition those of our existing customers subscribed to our historic packages over to the new service bundles.

Our service bundles are:

- M2A: Cyber Security and Resiliency with Archiving. This bundle includes Email Security with Targeted Threat Protection; Compliance Security; Continuity services and a 99-year archive.
- M2: Cyber Security and Resiliency. This bundle includes Email Security plus Targeted Threat Protection; Compliance Security and Continuity with 58-day email retention for recovery purposes.

Customers with specific projects or pre-defined business projects can also purchase the following additional services:

- S1: Advanced Threat Security. This service is designed to protect the organization against advanced threats such as whaling and spear-phishing with real-time URL blocking, attachment scanning and domain checking, as well as anti-malware and leading spam protection to shield employees and enhance productivity.
- S2: Advanced Threat Security with Internal Email Protect. This service contains the same features as S1 but also includes our latest addition to the Targeted Threat Protection family of products. Internal Email Protect offers detection of internal security threats and inspection of outbound emails plus, should any issue be detected, the remediation of such.
- D1: Data Leak Protection and Content Security. This service is designed to lock down sensitive corporate information with advanced data leak prevention, data leak detection, document and policy controls.
- C1: Mailbox Continuity. Our customers use this service to ensure that their email works even when the primary mail server is down. We continue sending and receiving email with a 100% uptime SLA with coverage for all mobile devices and web access.
- A1: Email Archiving. This service archives email and attachments in a fully-encrypted, independent, cloud data store separate from the mail environment.

Mimecast Mobile and Desktop Apps

Mobile, PC and Mac® users get self-service access to security features, including spam reporting and managed sender lists, the ability to send and receive email during a primary email system outage, and access to their personal email archive to run searches on its content. Administrators can use granular permissions to activate functions for individual employees or groups of users, while centralized security and policy management means IT teams can retain control over default settings.

Sales and Marketing

Our sales and marketing teams work together to build a strong sales pipeline, cultivate and retain customers and drive market awareness of our current and future products and services.

Sales

We sell our services through direct sales efforts and through our channel partners. Our sales model is designed to meet the needs of small and mid-market organizations and large enterprises across a wide range of industries and in over

130 countries. Our sales team is based in offices in Boston, Chicago, Dallas and San Francisco, United States; London, United Kingdom; Johannesburg and Cape Town, South Africa; Melbourne and Sydney, Australia; Amsterdam, the Netherlands, Dubai, UAE and Munich, Germany. We maintain a highly-trained sales force of approximately 350 employees as of March 31, 2018, which is responsible for acquiring and developing new business.

We also have an experienced sales team focused on developing and strengthening our channel partner relationships. Many organizations work with third-party IT channel partners to meet their security, IT and cloud service needs, so we have formed relationships with a variety of the leading partners to target large enterprises, mid-market and small organizations. For large enterprises, we work with international partners including CDW and Dimension Data. In the mid-market, we work with leading national partners, including Softchoice, SHI, CDW and Softcat. The small business market is primarily served by the reseller community and also by Managed Service Providers, who typically provide or host email services. We work closely with all of these channel partners to offer cooperative marketing, deal registration, as well as support and technical resources. We believe these partners view our services as a key source of additional revenue and a way for them to add significant value to their customers as they can support their desire to move to the cloud without compromising their security position.

Sales to our channel partners are generally subject to our standard, non-exclusive channel partner agreement, meaning our channel partners may offer customers the products of several different companies. These agreements are generally for a term of one year with a one-year renewal term and can be terminated by us or the channel partner. Payment to us from the channel partner is typically due within 30 calendar days of the date we issue an invoice for such sales.

Our sales cycle varies by size and sophistication of customer, the number of products purchased and the complexity of the project, ranging from several days for incremental sales to existing customers, to many months for sales to new customers or large deployments.

We plan to continue to invest in our sales organization to support both the growth of our direct sales organization and our channel partners.

Marketing

Our marketing strategy is designed to meet the specific needs of each of our customer segments. We are focused on building the Mimecast brand, product awareness, increasing customer adoption of our products, communicating the advantages of our solution and its benefit to organizations, and generating leads for our channel partners and direct sales force. We also invest in public relations and thought leadership to build our overall brand and visibility. We execute our marketing strategy by using a combination of internal marketing professionals and a network of global channel partners. We invest in field, channel, product and brand marketing and have increased our investment in digital marketing to drive greater lead generation volume and efficiency. Our local marketing teams support the conversion of these leads into qualified opportunities for inside sales and are responsible for branding, content generation and product marketing.

Customer Service and Support

We maintain our strong customer retention rate through the strength and quality of our products, our commitment to our customers' success and our award-winning global Customer Success and Support teams, which consist of more than 260 employees dedicated to ensuring a superior experience for our customers. For each of the fiscal years ended March 31, 2018, 2017 and 2016, our customer renewal rate has been consistently greater than 90%. We calculate our annual customer retention rate as the percentage of paying customers on the last day of the prior year who remain paying customers on the last day of the current year.

We have designed a comprehensive monitoring methodology that measures and evaluates the interactions we have with our customers from sales and on-boarding to support and renewal. Our cross-functional teams, under the supervision of our Chief of Customer Operations, work together to ensure the best customer experience is achieved and to address customer needs as they arise.

A key value driver of our customer on-boarding process is our Legacy Data Migration services. Our customers often have legacy email archives that they want to move to the cloud. Our data migration service helps solve the problems customers face when extracting data and getting it into the right format for importing to the cloud, which can be expensive, time-consuming and require interactions with multiple vendors.

In addition, we offer a full range of support services to our global customer base, including comprehensive online resources and email support with no outsourcing of support or account management to third parties. We also offer a range of additional services that include options for 24x7 telephone support and an assigned customer success manager. These support services are tiered to meet specific requirements of our diverse customers.

Our full range of customer outcome driven onboarding services is designed to cater to all customer segments. These services include dedicated implementation and onboarding consultancy services.

We have a dedicated training team and resources designed to enable customers to get the full benefit from their Mimecast investment. Our comprehensive education and consultancy offerings include administrator training and certification, end user training, and e-discovery training for compliance teams, all of which are available in-person and online.

Beyond customer support and training, we also provide a range of services that are designed to provide additional enablement to customers who require it, especially larger enterprises with more complex email infrastructure and legacy data. Our Success Planning and Professional Services teams work directly with the customer or partner to assist them in planning, migration and service activation.

We offer a service level agreement as part of our standard contract that contains commitments regarding the delivery of email messages to and from our servers, the speed at which our archive can produce search results, and our ability to correctly identify and isolate spam and viruses. If we do not achieve these levels, the customer can request a credit. Payment of the credit will be made subject to verification of the problem. These credits are tiered according to the extent of the service issued. The amount of credits provided to customers to date has been immaterial in all historical periods.

Customers

As of March 31, 2018, we had approximately 30,400 customers and protected millions of their employees in over 130 countries. Our diverse global footprint is evidenced by the fact that in the fiscal year ended March 31, 2018, we generated 49% of our revenue from the United States, 31% from the United Kingdom, 15% from South Africa and 5% from the rest of the world. Our customers range from large enterprises with over 75,000 employees to small organizations with less than 50 employees and represent a diverse set of industries. For example, in the fiscal year ended March 31, 2018, we generated 12% of our revenue from customers in the legal services industry, 14% from customers in the professional, scientific and technical services industry, 10% from customers in the manufacturing industry and 13% from customers in the finance and insurance industry. Our business is not dependent on any particular customer. No single customer represented more than 1% of our annual revenues in the fiscal years ended March 31, 2018, 2017 or 2016.

Research and Development

Our engineering, operations, product and development teams work together to enhance our existing products, technology infrastructure and underlying Mime | OS™ cloud architecture, as well as develop our new product pipeline. Our research and development team interacts with our customers and partners to address emerging market needs, counter developing threats and drive innovation in risk management and data protection. We operate a continuous delivery model for improvements to our infrastructure and products to ensure customers benefit from regular updates in protection and functionality without the need for significant intervention on their part. Our research and development efforts give prominence to services that enhance our unification commitment and allow customers to displace point solutions or on-premises products.

Our research and development expenses were $38.4 million, $22.6 million and $17.7 million for the fiscal years ended March 31, 2018, 2017 and 2016, respectively.

Intellectual Property

Our success is dependent, in part, on our ability to protect our proprietary technologies and other intellectual property rights. We primarily rely on a combination of trade secrets, copyrights and trademarks, as well as contractual protections to establish and protect our intellectual property rights. As of March 31, 2018, we have 12 patents issued

and 12 patent applications pending in the United States. We also have 4 patents issued and 5 patent applications pending for examination in non-U.S. jurisdictions. We intend to pursue additional patent protection to the extent that we believe it would be beneficial and cost effective.

We have registered “Mimecast” and certain other marks as trademarks in the United States and several other jurisdictions. We also have a number of registered and unregistered trademarks in the United States and certain other jurisdictions, and will pursue additional trademark registrations to the extent we believe it would be beneficial and cost effective. We are the registered holder of a variety of domestic and international domain names that include “mimecast.com,” “mimecast.co.uk,” “mimecast.co.za,” and similar variations.

In addition to the protection provided by our intellectual property rights, as part of our confidentiality procedures, all of our employees and independent contractors are required to sign agreements acknowledging that all inventions, trade secrets, works of authorship, developments and other processes generated by them on our behalf are our property, and they assign to us any ownership that they may claim in those works. We also generally enter into confidentiality agreements with our employees, consultants, partners, vendors and customers, and generally limit access to and distribution of our proprietary information.

Despite our precautions, it may be possible for unauthorized third parties to copy our products and use information that we regard as proprietary to create products and services that compete with ours. Some license provisions protecting against unauthorized use, copying, transfer and disclosures of our products may be unenforceable under the laws of certain jurisdictions and foreign countries. In addition, the laws of some countries do not protect proprietary rights to as great of an extent as the laws of the United States, and many foreign countries do not enforce these laws as diligently as government agencies and private parties in the United States. Our exposure to unauthorized copying and use of our products and misappropriation of our proprietary information may increase as a result of our foreign operations.

We expect that software and other solutions in our industry may be increasingly subject to third-party infringement claims as the number of competitors grows and the functionality of products in different industry segments overlap. Moreover, many of our competitors and other industry participants have been issued patents or filed patent applications, and have asserted claims and related litigation regarding patent and other intellectual property rights. Third parties, including non-practicing patent holders, have from time to time claimed, and could claim in the future, that our technologies infringe patents they now hold or might obtain or be issued in the future. See “Risk Factors — We may be sued by third parties for alleged infringement of their proprietary rights.”

Competition

Our market is large, highly competitive, fragmented, and subject to rapidly evolving technology and security threats, shifting customer needs and frequent introductions of new products and services. We do not believe that any specific competitor offers the fully unified service and integrated technology that we do. However, we do compete with companies that offer products that target email and data security, continuity and archiving, as well as large providers such as Google Inc. and Microsoft Corporation, who offer functions and tools as part of their core mailbox services that may be, or be perceived to be, similar to our offerings. Our current and potential future competitors include: Barracuda Networks, Inc., Google, Microsoft Exchange® Online Protection, Proofpoint, Inc., Symantec Corporation and Cisco Systems Inc., in security, and EMC, Microsoft Office 365®, Veritas Technologies LLC and Barracuda in archiving. Some of our current and future competitors may have certain competitive advantages such as greater name recognition, longer operating history, larger market share, larger existing user base and greater financial, technical and other resources. Some competitors may be able to devote greater resources to the development, promotion and sale of their products than we can to ours, which could allow them to respond more quickly than we can to new technologies, threats and changes in customer needs. We cannot provide any assurance that our competitors will not offer or develop products or services that are superior to ours or achieve greater market acceptance.

The principal competitive factors in our market include, but are not limited to:

- reliability and effectiveness in protecting, detecting and responding to cyberattacks;
- scalability and multi-tenancy of our system;
- breadth and unification of our services;
- cloud-only delivery;
- total cost of ownership;
- speed, availability and reliability;
- integration into office productivity, desktop and mobile tools;
- speed at which our services can be deployed;
- ease of user experience for IT administrators and employees; and
- superior customer service and commitment to customer success.

We believe that we compete favorably on the basis of these factors. Our ability to remain competitive will depend to a great extent upon our ongoing performance in the areas of product and cloud architecture development, core technical

innovation, channel management and customer support.

Employees

As of March 31, 2018, we had 1,192 employees and subcontractors, including 483 in sales and marketing, 256 in research and development, 260 in services and support and 193 in general and administrative. While we have operations in the United Kingdom, the United States, South Africa, Australia and Germany, most of our employees are based in the United Kingdom and the United States. None of our employees are represented by a labor union or covered by a collective bargaining agreement. We have never experienced a strike or similar work stoppage, and we consider our relations with our employees to be good.

Corporate Information

Mimecast Limited was incorporated under the laws of the Bailiwick of Jersey with company number 119119 on July 28, 2015 as a public company limited by shares. On November 4, 2015, Mimecast Limited became the holding company of Mimecast UK Limited, a private limited company incorporated in 2003 under the laws of England and Wales, and its subsidiaries by way of a share-for-share exchange in which the shareholders of Mimecast UK Limited exchanged their shares in Mimecast UK Limited for an identical number of shares of the same class in Mimecast Limited. Following the exchange, the historical consolidated financial statements of Mimecast UK Limited became the historical consolidated financial statements of Mimecast Limited, of which the consolidated financial statements as of and for the three years ended March 31, 2018 are included in this Annual Report on Form 10-K. Mimecast Limited has nine subsidiaries. Our principal operating companies are Mimecast UK Limited, a company organized under the laws of England and Wales, Mimecast Services Ltd, a company organized under the laws of England and Wales, Mimecast North America Inc., a Delaware, United States corporation, Mimecast South Africa (Pty) Ltd., a South African corporation, Mimecast Australia Pty. Ltd., an Australian corporation, and Mimecast Germany GmbH, a German corporation, each of which is a wholly-owned subsidiary of Mimecast Limited. Our principal executive office is located at CityPoint, One Ropemaker Street, Moorgate, London, EC2Y 9AW, United Kingdom.

Our ordinary shares are traded on The Nasdaq Global Select Market under the symbol “MIME”.

Geographic Information

For financial reporting purposes, total revenue and property and equipment, net attributable to geographic areas are presented in Note 14, “Segment and Geographic Information”, to the consolidated financial statements, included elsewhere in this Annual Report on Form 10-K.

Available Information

We maintain an Internet website at www.mimecast.com. The information on, or that can be accessed through, our website is not incorporated by reference into this Annual Report on Form 10-K and should not be considered to be a part of this Annual Report on Form 10-K. Our website address is included in this Annual Report on Form 10-K as inactive textual reference only. Our reports filed or furnished pursuant to Section 13(a) or 15(d) of the Securities Exchange Act of 1934, as amended, or the Exchange Act, including our Annual Reports on Form 10-K, our Quarterly Reports on Form 10-Q and our Current Reports on Form 8-K, and amendments to those reports, are accessible through our website, free of charge, as soon as reasonably practicable after these reports are filed electronically with, or otherwise furnished to, the Securities and Exchange Commission, or the SEC. We also make available on our website the charters of our audit committee, compensation committee and nominating and corporate governance committee, as well as our corporate governance guidelines and our code of business conduct and ethics. You may request copies of our reports and the other documents referenced above, at no cost, by writing to or telephoning us as follows:

Mimecast Limited

Attention: Robert Sanders

191 Spring Street

Lexington, Massachusetts 02421

Telephone: 617-393-7050

15

Item 1A. Risk Factors.

Our business, financial condition, results of operations and future growth prospects could be materially and adversely affected by the following risks or uncertainties. The risks and uncertainties described below are those that we have identified as material, but they are not the only risks and uncertainties we face. Our business is also subject to general risks and uncertainties that affect many other companies, including overall economic and industry conditions, as well as other risks not currently known to us or that we currently consider immaterial. If any of such risks and uncertainties actually occurs, our business, financial condition, results of operations and prospects could differ materially from the plans, projections and other forward-looking statements included in the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations" and elsewhere in this Annual Report on Form 10-K and in our other public filings.

Risks Related to Our Business and Our Industry

If we are unable to attract new customers and retain existing customers, our business and results of operations will be affected adversely.

To succeed, we must continue to attract new customers and retain existing customers who desire to use our security, continuity and archiving offerings. Acquiring new customers is a key element of our continued success, growth opportunity and future revenue. We will continue to invest in a direct sales force combined with a focused channel strategy designed to serve the various requirements of small, mid-market and large enterprises and to bring new customers onto our cloud architecture. Any failures by us to execute in these areas will negatively impact our business. The rate at which new and existing customers purchase our products depends on a number of factors, including those outside of our control. For example, in the fiscal year ended March 31, 2017, we benefited from the decision by Intel Corporation to end-of-life its McAfee MX Logic email protection product. Our future success also depends on retaining our current customers at acceptable retention levels. Our retention rates may decline or fluctuate as a result of a number of factors, some of which may be outside our control, including competition, customers' budgeting and spending priorities, and overall general economic conditions. If our customers do not renew their subscriptions for our products and services, our revenue would decline and our business would suffer. In future periods, our total customers and revenue could decline or grow more slowly than we expect.

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

A significant portion of our revenue growth is generated from sales of additional services and features to existing customers. Our future success depends, in part, on our ability to continue to sell such additional services and features to our existing customers. We devote significant efforts to developing, marketing and selling additional services and features and associated support services to existing customers and rely on these efforts for a portion of our revenue. These efforts require a significant investment in building and maintaining customer relationships, as well as significant research and development efforts in order to provide upgrades and launch new services and features. The rate at which our existing customers purchase additional services and features depends on a number of factors, including the perceived need for additional security, continuity and archiving, the efficacy of our current services, the perceived utility of our new offerings, our customers' IT budgets and general economic conditions. If our efforts to sell additional services and features to our customers are not successful, our future revenues and operating results will be harmed.

Failure to effectively expand our sales and marketing capabilities could harm our ability to acquire new customers and achieve broader market acceptance of our services.

Acquiring new customers and expanding sales to existing customers will depend to a significant extent on our ability to expand our sales and marketing operations. We generate approximately one-third of our revenue from direct sales and we expect to continue to rely on our sales force to obtain new customers and grow revenue from our existing customer base. We expect to expand our sales force in all of our regions and we face a number of challenges in achieving our hiring goals. For instance, there is significant competition for sales personnel with the sales skills and technical knowledge that we require. In addition, training and integrating a large number of sales and marketing personnel in a short period of time requires the allocation of significant internal resources. Our ability to achieve projected growth in revenue in the future will depend, in large part, on our success in recruiting, training and retaining sufficient numbers of sales personnel. We invest significant time and resources in training new sales personnel to understand our solutions and growth strategy. In general, new hires require significant training and substantial experience before becoming productive. Our recent hires and planned hires may not become as productive as we require, and we may be unable to hire or retain sufficient numbers of qualified individuals in the future in the markets where we currently operate or where we seek to conduct business. Our growth may be materially and adversely impacted if the efforts to expand our sales and marketing capabilities are not successful or if they do not generate a sufficient increase in revenue.

Our business depends substantially on customers renewing their subscriptions with us. A decline in our customer renewals would harm our future operating results.

In order for us to maintain or improve our operating results, it is important that our customers renew their subscriptions with us when the existing subscription term expires. Although the majority of our customer contracts include auto-renew provisions, our customers have no obligation to renew their subscriptions upon expiration, and we cannot provide assurance that customers will renew subscriptions at the same or higher level of service, if at all. For each of the fiscal years ended March 31, 2018, 2017 and 2016, our customer retention rate has been consistently greater than 90%. We calculate customer retention rate as the percentage of paying customers on the last day of the relevant period in the prior year who remain paying customers on the last day of the relevant period in the current year. The rate of customer renewals may decline or fluctuate as a result of a number of factors, including our customers' satisfaction or dissatisfaction with our solutions, the effectiveness of our customer support services, our pricing, the prices of competing products or services, mergers and acquisitions affecting our customer base, or reductions in our customers' spending levels. If our customers do not renew their subscriptions, or renew on less favorable terms, our revenue may decline, and we may not realize improved operating results from our customer base.

The markets in which we participate are highly competitive, with several large established competitors, and our failure to compete successfully would make it difficult for us to add and retain customers and would reduce or impede the growth of our business.

Our market is large, highly competitive, fragmented and subject to rapidly evolving technology, shifting customer needs and frequent introductions of new products and services. We currently compete with companies that offer products that target email and data security, continuity and archiving, as well as large providers such as Google Inc. and Microsoft Corporation, which offer functions and tools as part of their core mailbox services that may be, or be perceived to be, similar to ours. Our current and potential future competitors include: Barracuda Networks, Inc., Google, Microsoft Exchange Online Protection, Proofpoint, Inc., Symantec Corporation and Cisco Systems Inc., in security, and EMC, Microsoft Office 365®, Veritas Technologies LLC and Barracuda in archiving. We expect competition to increase in the future from both existing competitors and new companies that may enter our markets. Additionally, some potential customers, particularly large enterprises, may elect to develop their own internal products. If two or more of our competitors were to merge or partner with one another, the change in the competitive landscape could reduce our ability to compete effectively. Our continued success and growth depends on our ability to out-perform our competitors at the individual service level as well as increasing demand for a unified service infrastructure. We cannot guarantee that we will out-perform our competitors at the product level or that the demand for a unified service technology will increase.

Some of our current competitors have, and our future competitors may have, certain competitive advantages such as greater name recognition, longer operating history, larger market share, larger existing user base and greater financial, technical and other resources. Some competitors may be able to devote greater resources to the development, promotion and sale of their products and services than we can to ours, which could allow them to respond more quickly than we can to new technologies and changes in customer needs. We cannot assure you that our competitors will not offer or develop products or services that are superior to ours or achieve greater market acceptance.

Data security and integrity are critically important to our business, and breaches of our information and technology networks and unauthorized access to a customer's data could harm our business and operating results.

We have experienced, and will continue to experience, cyberattacks and other malicious internet-based activity, which continue to increase in sophistication, frequency and magnitude. Because our services involve the storage of large amounts of our customers' sensitive and proprietary information, solutions to protect that information from cyberattacks and other threats, data security and integrity are critically important to our business. Despite all of our

efforts to protect this information, we cannot provide assurance that systems that access our services and databases will not be compromised or disrupted, whether as a result of criminal conduct, distributed denial of service, or DDoS, attacks, such as the one we experienced in September 2015, or other advanced persistent attacks by malicious actors, including hackers, state-backed hackers and cybercriminals, breaches due to employee error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural disasters or other catastrophic events. Because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently or may be designed to remain dormant until a predetermined event and often are not recognized until launched against a target, we may be unable to anticipate these techniques or implement adequate preventative measures. Though it is difficult to determine what harm may directly result from any specific interruption or breach, unauthorized access to or disclosure of confidential information, disruption, including DDoS attacks, or the perception that the confidential information of our customers is not secure, any of these events could result in a material loss of business, substantial legal liability or significant harm to our reputation. Further, any mandatory regulatory disclosures regarding a security breach, unauthorized access to or disclosure of confidential information often lead to widespread negative publicity, which may cause our customers to lose confidence in the effectiveness of our data security measures.

We must continually monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access and expend significant resources to respond to threats to security. However, despite our efforts, we may fail to identify these new and complex methods of attack, or fail to invest sufficient resources in security measures. In addition, as we increase our customer base and our brand becomes more widely known and recognized, we may become more of a target for malicious third parties. Any breach of our security measures as a result of third-party action, employee negligence and/or error, malfeasance, defects or otherwise that compromises the confidentiality, integrity or availability of our data or our customers' data could result in:

- severe harm to our reputation or brand, or materially and adversely affect the overall market perception of the security and reliability of our services;
- individual customer and/or class action lawsuits, which could result in financial judgments against us and which would cause us to incur legal fees and costs;
- legal or regulatory enforcement action, which could result in fines and/or penalties and which would cause us to incur legal fees and costs; and/or
- additional costs associated with responding to the interruption or security breach, such as investigative and remediation costs, the costs of providing individuals and/or data owners with notice of the breach, legal fees, the costs of any additional fraud detection activities, or the costs of prolonged system disruptions or shutdowns.

Any of these events could materially adversely impact our business and results of operations.

Data privacy concerns, evolving regulations of cloud computing, cross-border data transfer restrictions and other domestic or foreign laws and regulations may limit the use and adoption of, or require modification of, our products and services, which could limit our ability to attract new customers or support existing customers thus reducing our revenues, harming our operating results and adversely affecting our business.

Laws and regulations related to the provision of services on the Internet are increasing, as federal, state and foreign governments continue to adopt new laws and regulations addressing data privacy and the collection, processing, storage and use of personal information. For example, in the United States, these include laws and regulations promulgated under the authority of the Federal Trade Commission, the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, the Health Insurance Portability and Accountability Act of 1996, or HIPAA, the Graham-Leach-Bliley Act of 1999, or Gramm-Leach-Bliley, and state breach notification laws, as well as regulator enforcement positions and expectations reflected in federal and state regulatory actions, settlements, consent decrees and guidance documents. Internationally, virtually every jurisdiction in which we operate has established its own data security and privacy legal frameworks with which we, or our customers, must comply, including the Data Protection Directive 95/46/EC, or the Directive, established in the European Union, or EU, and local EU Member State legislation implementing the Directive, such as the Data Protection Act in the United Kingdom. Most recently, the EU adopted the EU General Data Protection Regulation, or GDPR, which became effective on May 25, 2018 and replaced the Directive. The GDPR applies to any company established in the EU as well as to those outside the EU if they collect and use personal data in connection with the offering of goods or services to individuals in the EU or the monitoring of their behavior. The GDPR enhances data protection obligations for processors and controllers of personal data, including, for example, expanded disclosures about how personal information is to be used, limitations on retention of information, mandatory data breach notification requirements and onerous new obligations on services providers. Under the GDPR, fines of up to 20,000,000 Euros or up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, may be imposed. Given the breadth and depth of changes in data protection obligations, complying with its requirements has caused us to expend significant resources and such expenditures are likely to continue into the near future as we respond to new interpretations and enforcement actions that may follow the effective date of the regulation and as we continue to negotiate data processing agreements with our customers and business partners.

To facilitate and legitimize the transfer of both customer and personnel data from the European Union to the United States, in the past we have relied on the EU-U.S. Safe Harbor Framework, which required U.S.-based companies to provide assurance that they were adhering to relevant European standards for data protection. On October 6, 2015, the Court of Justice of the European Union invalidated the EU-U.S. Safe Harbor Framework. On February 2, 2016, the U.S. and EU announced agreement on a new framework for transatlantic data flows entitled the EU-U.S. Privacy Shield and we self-certified under the EU-US Privacy Shield framework in March 2018. However, the Privacy Shield continues to be subject to legal challenges and, as a result, there is some uncertainty regarding its future validity and our ability to rely on it for EU to US data transfers. If the Privacy Shield is ultimately invalidated, we will be required to identify and implement alternative solutions to ensure that we are in compliance with European data transfer requirements. If we fail to comply fully with European privacy laws, EU data protection authorities might impose upon us a number of different sanctions, including fines and restrictions on transfers.

Privacy and data protections laws and regulations are subject to new and differing interpretations and there may be significant inconsistency in laws and regulations among the jurisdictions in which we operate or offer our SaaS solutions. Legal and other regulatory requirements could restrict our ability to store and process data as part of our SaaS solutions, or, in some cases, impact our ability to offer our SaaS products in certain jurisdictions. Such laws may also impact our customers' ability to deploy certain of our solutions globally, to the extent they utilize our products for storing personal information that they store and process. In addition, in many cases these privacy laws apply not only to transfers of information to third parties, but also within an enterprise, including our company or our customers. Additionally, if third parties that we work with, violate applicable laws or our policies, such violations may also put our customers' information at risk and could in turn have an adverse effect on our business. The costs of compliance with, and other burdens imposed by, data privacy laws, regulations and standards may require resources to create new products or modify existing products, could lead to us being subject to significant fines, penalties or liabilities for noncompliance, and may slow the pace at which we close sales transactions, any of which could harm our business.

If we are unable to effectively increase sales of our services to large enterprises while mitigating the risks associated with serving such customers, our business, financial position and results of operations may suffer.

As we seek to increase our sales to large enterprise customers, we may face longer sales cycles, more complex customer requirements, unfavorable contractual terms, substantial upfront sales costs and less predictability in completing some of our sales than we do with smaller customers. In addition, our ability to successfully sell our services to large enterprises is dependent on us attracting and retaining sales personnel with experience in selling to large organizations. Also, because security breaches of larger, more high-profile enterprises are likely to be heavily publicized, there is increased reputational risk associated with serving such customers. If we are unable to increase sales of our services to large enterprise customers while mitigating the risks associated with serving such customers, our business, financial position and results of operations may suffer.

If we are unable to maintain successful relationships with our channel partners, our ability to acquire new customers could be adversely affected.

In order to grow our business, we anticipate that we will continue to depend on our relationships with our channel partners who we rely on, in addition to our direct sales force, to sell and support our services. In our fiscal year ended March 31, 2018, while no individual channel partner accounted for 10% or more of our sales, in the aggregate, our channel partners accounted for 69% of our sales. We expect that sales to channel partners will continue to account for a substantial portion of our revenue for the foreseeable future. We utilize channel partners to efficiently increase the scale of our marketing and sales efforts, increasing our market penetration to customers which we otherwise might not reach on our own. Our ability to achieve revenue growth in the future will depend, in part, on our success in maintaining successful relationships with our channel partners.

Our agreements with our channel partners are generally non-exclusive, meaning our channel partners may offer customers competitive services from different companies. If our channel partners do not effectively market and sell our services, choose to use greater efforts to market and sell their own products or services or those of others, or fail to meet the needs of our customers, our ability to grow our business, sell our services and maintain our reputation may be adversely affected. Our agreements with our channel partners generally allow them to terminate their agreements for any reason upon 90 days' notice. The loss of key channel partners, our possible inability to replace them, or the failure to recruit additional channel partners could materially adversely affect our results of operations. If we are unable to maintain our relationships with these channel partners, our business, results of operations, financial condition or cash flows could be adversely affected.

We provide service level commitments under our subscription agreements and service disruptions could obligate us to provide refunds and we could face subscription terminations, which could adversely affect our revenue.

Our subscription agreements with customers provide certain service level commitments. If we are unable to meet the stated service level commitments or suffer extended periods of downtime that exceed the periods allowed under our customer agreements, we could be required to pay refunds or face subscription terminations, either of which could significantly impact our revenue.

To date, we have suffered two significant service disruptions. The first occurred in 2013 and was a result of an equipment failure. Many of our customers in the United Kingdom experienced service disruptions for several hours. We also experienced a service disruption in September 2015 as a result of an external network DDoS attack. Customers using our Secure Email Gateway service in the United States experienced downtime related to the delivery and receipt of external emails for several hours. The scope of the incident was limited to network traffic and no customer data was lost or compromised. As a result of the service disruption, we voluntarily provided service credits to affected customers in the year ended March 31, 2016, totaling approximately $0.4 million. While we have undertaken substantial remedial efforts to prevent future incidents like these, we cannot guarantee that future attacks or service disruptions will not occur. Any future attacks or service disruptions could adversely affect our reputation, our relationships with our existing customers and our ability to attract new customers, all of which would impact our future revenue and operating results.

If we are not able to provide successful updates, enhancements and features to our technology to, among other things, keep up with emerging cyber-threats and customer needs, our business could be adversely affected.

Our industry is marked by rapid technological developments and demand for new and enhanced services and features to meet the evolving IT needs of organizations. In particular, cyber-threats are becoming increasingly sophisticated and responsive to the new security measures designed to thwart them. If we fail to identify and respond to new and increasingly complex methods of attack and update our products to detect or prevent such threats, our business and reputation will suffer. The success of any new enhancements, features or services that we introduce depends on several factors, including the timely completion, introduction and market acceptance of such enhancements, features or services. We may not be successful in either developing these modifications and enhancements or in bringing them to market in a timely fashion. Furthermore, modifications to existing technologies will increase our research and development expenses. If we are unable to successfully enhance our existing services to meet customer requirements, increase adoption and usage of our services, or develop new services, enhancements and features, our business and operating results will be harmed.

Because we recognize revenue from subscriptions for our services over the term of the agreement, downturns or upturns in new business may not be immediately reflected in our operating results and may be difficult to discern.

We generally recognize subscription revenue from customers ratably on a straight-line basis over the terms of their subscription agreements, which are typically one year in duration. As a result, most of the revenue we report in each quarter is derived from the recognition of deferred revenue relating to subscription agreements entered into during the previous fiscal year or quarter. Consequently, a decline in new or renewed subscriptions with yearly terms in any one quarter may have a small impact on our operating revenue results for that quarter. However, such decline will negatively affect our revenue in future quarters. Accordingly, the effect of significant downturns in sales and market acceptance of our services, and potential changes in our pricing policies, rate of expansion or retention rate may not be fully reflected in our operating results until future periods. Shifts in the mix of annual versus monthly subscription billings may also make it difficult to assess our business. We may also be unable to reduce our cost structure in line with a significant deterioration in sales. In addition, a significant majority of our costs are expensed as incurred, while revenue is recognized over the life of the agreement with our customer. As a result, increased growth in the number of our customers could continue to result in our recognition of more costs than revenue in the earlier periods of the terms of our agreements. Our subscription model also makes it difficult for us to rapidly increase our revenue through additional sales in any period, as revenue from new customers is recognized over the applicable subscription term.

We have incurred losses in the past, and we may not be able to achieve or sustain profitability for the foreseeable future.

We have incurred losses in each period since our inception in 2003 up through our fiscal year ended March 31, 2018, with the exception of our fiscal year ended March 31, 2015 in which we generated net income of $0.3 million. In our fiscal years ended March 31, 2018 and 2017, we incurred a net loss of $12.4 million and $5.4 million, respectively. As of March 31, 2018, we had an accumulated deficit of $106.5 million. We have been growing rapidly, and, as we do so, we incur significant sales and marketing, support and other related expenses. Our ability to achieve and sustain profitability will depend in significant part on our obtaining new customers, expanding our existing customer relationships and ensuring that our expenses, including our sales and marketing expenses and the cost of supporting new customers, does not exceed our revenue. We also expect to make significant expenditures and investments in research and development to expand and improve our services and technical infrastructure. In addition, as a public company, we expect to continue to incur significant legal, accounting and other expenses that we did not incur prior to our initial public offering in November 2015. These increased expenditures may make it harder for us to achieve and maintain profitability and we cannot predict when we will achieve sustained profitability, if at all. We also may incur losses in the future for a number of other unforeseen reasons. Accordingly, we may not be able to maintain

profitability, once achieved, and we may incur losses in the foreseeable future.

We are subject to a number of risks associated with global sales and operations.

We operate a global business with offices located in the United States, the United Kingdom, South Africa, Australia and Germany. In the fiscal year ended March 31, 2018, we generated 49% of our revenue from the United States, 31% from the United Kingdom, 15% from South Africa and 5% from the rest of the world. As a result, our sales and operations are subject to a number of risks and additional costs, including the following:

- fluctuations in exchange rates between currencies in the markets where we do business;
- risks associated with trade restrictions and additional legal requirements, including the exportation of our technology that is required in some of the countries in which we operate;
- greater risk of unexpected changes in regulatory rules, regulations and practices, tariffs and tax laws and treaties;

- compliance with multiple anti-bribery laws, including the United States Foreign Corrupt Practices Act and the U.K. Anti-Bribery Act;
- 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;
- limited or uncertain protection of intellectual property rights in some countries and the risks and costs associated with monitoring and enforcing intellectual property rights abroad;
- greater difficulty in enforcing contracts and managing collections in certain jurisdictions, as well as longer collection periods;
- management communication and integration problems resulting from cultural and geographic dispersion;
- social, economic and political instability, terrorist attacks and security concerns in general; and
- potentially adverse tax consequences.

For example, in June 2016, the United Kingdom held a referendum in which a majority of voters approved an exit from the EU, or Brexit, and in March 2017, the United Kingdom formally notified the EU of its intention to withdraw from the EU. A two-year period has now commenced during which the United Kingdom and the EU will negotiate the future terms of the United Kingdom's relationship with the EU, including, among other things, the terms of trade between the United Kingdom and the EU. Brexit may affect our results of operations in a number of ways, including increasing currency exchange risk, generating instability in the global financial markets or negatively impacting the economies of the United Kingdom or Europe. In addition, because of our significant presence in the United Kingdom, it is possible that Brexit may require us to restructure some or all of our operations. The long-term effects of Brexit will depend in part on any agreements the United Kingdom makes to retain access to markets in the EU following the withdrawal from the EU. In addition, we expect that Brexit could lead to legal uncertainty and potentially divergent national laws and regulations as the United Kingdom determines which EU laws to replicate or replace. These and other factors could harm our ability to generate future global revenue and, consequently, materially impact our business, results of operations and financial condition.

These and other factors could harm our ability to generate future global revenue and, consequently, materially impact our business, results of operations and financial condition.

Fluctuations in currency exchange rates could adversely affect our business.

Our functional currency and that of our subsidiaries is the local currency of each entity and our reporting currency is the U.S. dollar. In our fiscal year ended March 31, 2018, 51% of our revenue was denominated in U.S. dollars, 29% in British pounds, 15% in South African rand and 5% in other currencies. Given that our functional currency and that of our subsidiaries is the local currency of each entity, but our reporting currency is the U.S. dollar, fluctuations in currency exchange rates between the U.S. dollar, the British pound, the South African rand and the Australian dollar could materially and adversely affect our business. There may be instances in which costs and revenue will not be matched with respect to currency denomination. We estimate that a 10% increase or decrease in the value of the British pound against the U.S. dollar would have increased or decreased our loss from operations by approximately $1.8 million in our fiscal year ended March 31, 2018 and that a 10% increase or decrease in the value of the South African rand against the U.S. dollar would have decreased or increased our loss from operations by approximately $2.4 million in our fiscal year ended March 31, 2018. To date, we have not entered into any currency hedging contracts. As a result, to the extent we continue our expansion on a global basis, we expect that increasing portions of our revenue, cost of revenue, assets and liabilities will be subject to fluctuations in currency valuations. We may experience economic loss and a negative impact on earnings or net assets solely as a result of currency exchange rate fluctuations.

Brexit may continue to have a significant impact on currency exchange rates and the global and European economy generally. The outcome of the referendum caused volatility in global stock markets and foreign currency exchange rate fluctuations, including the strengthening of the U.S. dollar against the British pound and the euro, which may continue or worsen as the outcome of the negotiations between the United Kingdom and the EU becomes clear.

We are dependent on the continued services and performance of our two founders, the loss of either of whom could adversely affect our business.

Our future performance depends upon contributions from our senior management team and, in particular, our two founders, Peter Bauer, our Chairman and Chief Executive Officer, and Neil Murray, our Chief Technology Officer. If our senior management team, including any new hires that we may make, fails to work together effectively and to execute on our plans and strategies on a timely basis, our business could be harmed. The loss of one or more of our executive officers or key employees could have an adverse effect on our business. The loss of services of either Mr. Bauer or Mr. Murray could significantly delay or prevent the achievement of our development and strategic objectives.

We depend on highly skilled personnel to grow and operate our business, and if we are unable to hire, retain and motivate qualified personnel, we may not be able to grow effectively.

Our success depends largely upon our continued ability to identify, hire, develop, motivate and retain highly skilled personnel, including senior management, engineers, software developers, sales representatives and customer support representatives. Our growth strategy also depends, in part, on our ability to continue to attract and retain highly skilled personnel. Identifying, recruiting, training and integrating qualified individuals requires significant time, expense and attention of management. Competition for these personnel is intense, especially for engineers experienced in designing and developing software and software as a service, or SaaS, applications, and for experienced sales professionals. We have, from time to time experienced, and we expect to continue to experience, difficulty in hiring and retaining employees with appropriate qualifications. Many of the companies with which we compete for experienced personnel have greater resources than we have. If we hire employees from competitors or other companies, their former employers may assert that these employees or we have breached their legal obligations, resulting in a diversion of our time and resources. In addition, prospective and existing employees often consider the value of the equity awards they receive in connection with their employment. If the actual or perceived value of our equity awards declines, or experiences significant volatility, it may adversely affect our ability to recruit and retain key employees. If we are not able to effectively recruit and retain qualified employees, our ability to achieve our strategic objectives will be adversely impacted, and our business will be harmed.

Any serious disruptions in our services caused by defects in our software or otherwise may cause us to lose revenue and market acceptance.

Our customers use our services for the most critical aspects of their business, and any disruptions to our services or other performance problems with our services, however caused, could hurt our brand and reputation and may damage our customers' businesses. We provide regular updates, which may contain undetected errors when first introduced or released. In the past, we have discovered software errors, failures, vulnerabilities and bugs in our services after they have been released and new errors in our existing services may be detected in the future. Real or perceived errors, failures, system delays, interruptions, disruptions or bugs could result in negative publicity, loss of or delay in market acceptance of our services, loss of competitive position, delay of payment to us, lower renewal rates, or claims by customers for losses sustained by them. In such an event, we may be required, or may choose, for customer relations or other reasons, to expend additional resources in order to mitigate or correct the problem. We seek to cap the liability to which we are exposed in the event of losses or harm to our customers, but we cannot be certain that we will obtain these caps or that these caps, if obtained, will be enforced in all instances. We carry insurance; however, the amount of such insurance may be insufficient to compensate us for any losses that may result from claims arising from defects or disruptions in our services. As a result, we could lose future sales and our reputation and our brand could be harmed.

If the prices we charge for our services are unacceptable to our customers, our operating results will be harmed.

As the market for our services matures, or as new or existing competitors introduce new products or services that compete with ours, we may experience pricing pressure and be unable to renew our agreements with existing customers or attract new customers at prices that are consistent with our pricing model and operating budget. If this were to occur, it is possible that we would have to change our pricing model or reduce our prices, which could harm our revenue, gross margin and operating results. Pricing decisions may also impact the mix of adoption among our subscription plans and negatively impact our overall revenue. Moreover, large enterprises, which may account for a larger portion of our business in the future, may demand substantial price concessions. If we are, for any reason, required to reduce our prices, our revenue, gross margin, profitability, financial position and cash flow may be adversely affected.

Our research and development efforts may not produce new services or enhancements to existing services that result in significant revenue or other benefits in the near future, if at all.

We invested 15%, 12% and 12% of our revenue in research and development in our fiscal years ended March 31, 2018, 2017 and 2016, respectively. We expect to continue to dedicate significant financial and other resources to our research and development efforts in order to maintain our competitive position. However, investing in research and development personnel, developing new services and enhancing existing services is expensive and time-consuming, and there is no assurance that such activities will result in significant new marketable services, enhancements to existing services, design improvements, cost savings, revenue or other expected benefits. If we spend significant time and effort on research and development and are unable to generate an adequate return on our investment, our business and results of operations may be materially and adversely affected.

We have acquired, and may acquire in the future, other businesses, products or technologies, which could require significant management attention, disrupt our business, dilute shareholder value and adversely affect our results of operations.

As part of our business growth strategy and in order to remain competitive, we may acquire, or make investments in, complementary companies, products or technologies. For example, in fiscal 2017, we acquired substantially all of the business of iSheriff, Inc., a cloud security provider, and in fiscal 2018, we acquired machine learning-based malware detection technology. Nevertheless, our acquisition experience to date remains limited, and as a result, our ability as an organization to acquire and integrate other companies, products or technologies in a successful manner is unproven. We may not be able to find suitable acquisition targets, and we may not be able to complete such acquisitions on favorable terms, if at all. If we do complete acquisitions, we may not ultimately strengthen our competitive position or achieve our goals, and any acquisitions we complete could be viewed negatively by our customers, analysts and investors. In addition, if we are unsuccessful at integrating such acquisitions or the technologies associated with such acquisitions, our revenue and results of operations could be adversely affected. In addition, while we will make significant efforts to address any information technology security issues with respect to any acquisitions, we may still inherit such risks when we integrate the acquired products and systems. Any integration process may require significant time and resources, and we may not be able to manage the process successfully. We may not successfully evaluate or utilize the acquired technology or personnel, or accurately forecast the financial impact of an acquired business, including accounting charges. We may have to pay cash, incur debt or issue equity securities to pay for any such acquisitions, each of which could adversely affect our financial condition or the value of our ordinary shares. The sale of equity or issuance of debt to finance any such acquisitions could result in dilution to our shareholders. The incurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations.

We employ third-party licensed software for use in or with our services, and the inability to maintain these licenses or errors in the software we license could result in increased costs, or reduced service levels, which would adversely affect our business.

Our services incorporate and rely on certain third-party software obtained under licenses from other companies. We anticipate that we will continue to rely on such third-party software and development tools in the future. Although we believe that there are commercially reasonable alternatives to the third-party software we currently license, this may not always be the case, or it may be difficult or costly to replace. In addition, integration of the software used in our services with new third-party software may require significant work and require substantial investment of our time and resources and delays in the release of our services until equivalent technology is either developed by us, or, if available, is identified, obtained and integrated, which could harm our business. A licensor may have difficulties keeping up with technological changes or may stop supporting the software or other intellectual property that it licensed to us. Also, to the extent that our services depend upon the successful operation of third-party software in conjunction with our software, any undetected errors or defects in this third-party software could prevent the deployment or impair the functionality of our services, delay new services introductions, result in a failure of our services, and injure our reputation. Our use of additional or alternative third-party software would require us to enter into additional license agreements with third parties on terms that may not be favorable to us.

If the market for SaaS business software applications develops more slowly than we expect or declines, our business would be adversely affected.

The expansion of the SaaS business applications market depends on a number of factors, including the cost, performance and perceived value associated with SaaS, as well as the ability of SaaS providers to address data security and privacy concerns. Additionally, government agencies have adopted, or may adopt, laws and regulations regarding the collection and use of personal information obtained from consumers and other individuals, or seek to

access information on our platform, either of which may reduce the overall demand for our platform. If we or other SaaS providers experience data security incidents, loss of customer data, disruptions in delivery, or other problems, the market for SaaS business applications, including our services, may be negatively affected.

Natural disasters, power loss, telecommunications failures and similar events could cause interruptions or performance problems associated with our information and technology infrastructure that could impair the delivery of our services and harm our business.

We currently store our customers' information within twelve third-party data center hosting facilities located in twelve locations around the world. As part of our current disaster recovery arrangements, our production environment and all of our customers' data is currently replicated in near real-time in a facility located in a different location. We cannot provide assurance that the measures we have taken to eliminate single points of failure will be effective to prevent or minimize interruptions to our operations. Our facilities are vulnerable to interruption or damage from a number of sources, many of which are beyond our control, including floods, fires, power loss, telecommunications failures and similar events. They may also be subject to break-ins, sabotage, intentional acts of vandalism and similar misconduct. Any damage to, or failure of, our systems generally could result in interruptions in our service. Interruptions in our service may reduce our revenue, cause customers to terminate their subscriptions and adversely affect our renewal

rate and our ability to attract new customers. Our business and reputation will also be harmed if our existing and potential customers believe our service is unreliable. The occurrence of a natural disaster, an act of terrorism, a decision to close the facilities without adequate notice or other unanticipated problems at these facilities could result in lengthy interruptions in our service. Even with the disaster recovery arrangements, our service could be interrupted. As we continue to add data centers and add capacity in our existing data centers, we may move or transfer our data and our customers' data. Any unsuccessful data transfers may impair the delivery of our service. Further, as we continue to grow and scale our business to meet the needs of our customers, additional burdens may be placed on our hosting facilities.

We are a multinational organization faced with increasingly complex tax issues in many jurisdictions, and we could be obligated to pay additional taxes in various jurisdictions.

As a multinational organization, we may be subject to taxation in several jurisdictions around the world with increasingly complex tax laws, the application of which can be uncertain. The amount of taxes we pay in these jurisdictions could increase substantially as a result of changes in the applicable tax principles, including increased tax rates, new tax laws or revised interpretations of existing tax laws and precedents, which could have a material adverse effect on our liquidity and results of operations. In addition, the authorities in these jurisdictions could review our tax returns and impose additional tax, interest and penalties, and the authorities could claim that various withholding requirements apply to us or our subsidiaries or assert that benefits of tax treaties are not available to us or our subsidiaries. Furthermore, one or more jurisdictions in which we do not believe we are currently subject to tax payment, withholding, or filing requirements, could assert that we are subject to such requirements. Any of these claims or assertions could have a material impact on us and the results of our operations.

We are subject to governmental export controls and funds dealings restrictions that could impair our ability to compete in certain international markets and subject us to liability if we are not in full compliance with applicable laws.

Our software and services may be subject to export controls and we may also be subject to restrictions or prohibitions on transactions with, or on dealing in funds transfers to/from, certain embargoed jurisdictions and sanctioned persons and entities, pursuant to the U.K. Export Control Organisation's restrictions, the U.K. Treasury's restrictions, the EU Council Regulations, the United States Department of Commerce's Export Administration Regulations, the economic and trade sanctions regulations administered by the United States Treasury Department's Office of Foreign Assets Controls and United States Department of State, and similar laws that may apply in other jurisdictions in which we operate or sell or distribute our services. Export control and economic sanctions laws include prohibitions on the sale or supply of certain products and services to certain embargoed or sanctioned countries, regions, governments, persons and entities, as well as restrictions or prohibitions on dealing in funds to/from those countries, regions, governments, persons and entities. In addition, various countries regulate the import of certain encryption items and technology through import permitting and licensing requirements, and have enacted laws that could limit our ability to distribute our services or could limit our customers' ability to implement our services in those countries.

The exportation, re-exportation, and importation of our software and services, including by our channel partners, must comply with applicable laws or else we may be adversely affected, through reputational harm, government investigations, penalties, and/or a denial or curtailment of our ability to export our services. Although we take precautions to prevent our services from being provided in violation of such laws, our services may have been in the past, and could in the future be, provided in violation of such laws.

If we are found to be in violation of U.S. sanctions or export control laws, it could result in substantial fines and penalties for us and for the individuals working for us, including civil penalties of up to $250,000 or twice the value of the transaction, whichever is greater, per violation, and in the event of conviction for a criminal violation, fines of up

to $1 million and possible incarceration for responsible employees and managers for willful and knowing violations. Under the terms of applicable regulations, each instance in which a company provides goods or services may be considered a separate violation. If we are found to be in violation of U.K. sanctions or export controls, it could also result in unlimited fines for us and responsible employees and managers, as well as imprisonment of up to two years for responsible employees and managers.

Changes in our software or services, or changes in export, sanctions or import laws, may delay the introduction and sale of our services in international markets, prevent our customers with international operations from deploying our software or services or, in some cases, prevent the export or import of our software or services to certain countries, regions, governments, persons or entities altogether, which could adversely affect our business, financial condition and operating results.

Our quarterly results may fluctuate for a variety of reasons and may not fully reflect the underlying performance of our business.

Our quarterly operating results, including the levels of our revenue, gross margin, profitability, cash flow and deferred revenue, may vary significantly in the future, and period-to-period comparisons of our operating results may not be meaningful. Accordingly, the results of any one quarter should not be relied upon as an indication of future performance. Our quarterly financial results may fluctuate as a result of a variety of factors, many of which are outside of our control and, as a result, may not fully reflect the underlying performance of our business. Fluctuations in quarterly results may negatively impact the value of our ordinary shares. Factors that may cause fluctuations in our quarterly financial results include, but are not limited to:

- foreign exchange rates;
- our ability to attract new customers;
- our revenue retention rate;
- the amount and timing of operating expenses related to the maintenance and expansion of our business, operations and infrastructure;
- network outages or security breaches;
- general economic, industry and market conditions;
- increases or decreases in the number of features in our services or pricing changes upon any renewals of customer agreements;
- changes in our pricing policies or those of our competitors;
- new variations in sales of our services, which has historically been highest in the fourth quarter of a given fiscal year;
- the timing and success of new services and service introductions by us and our competitors or any other change in the competitive dynamics of our industry, including consolidation among competitors, customers or strategic partners; and
- the impact of acquisitions.

If we need to raise additional capital to expand our operations and invest in new technologies in the future and cannot raise it on acceptable terms or at all, our ability to compete successfully may be harmed.

We believe that our existing cash and cash equivalents will be sufficient to meet our anticipated cash requirements for at least the next twelve months. However, unforeseen circumstances may arise which may mean that we may need to raise additional funds, and we may not be able to obtain additional debt or equity financing on favorable terms, if at all. If we raise additional equity financing, our security holders may experience significant dilution of their ownership interests and the value of our ordinary shares could decline. If we engage in debt financing, we may be required to accept terms that restrict our ability to incur additional indebtedness, force us to maintain specified liquidity or other ratios or restrict our ability to pay dividends or make acquisitions. If we need additional capital and cannot raise it on acceptable terms, if at all, we may not be able to, among other things:

- develop and enhance our services;
- continue to expand our research and development, sales and marketing organizations;
- hire, train and retain key employees;
- respond to competitive pressures or unanticipated working capital requirements; or
- pursue acquisition opportunities.

Our inability to do any of the foregoing could reduce our ability to compete successfully and harm our results of operations.

Risks Related to Intellectual Property

Any failure to protect our intellectual property rights could impair our ability to protect our proprietary technology and our brand.

Our success and ability to compete depend in part on our intellectual property. We primarily rely on copyright, trade secret and trademark laws, trade secret protection and confidentiality or license agreements with our employees, customers, partners and others to protect our intellectual property rights. However, the steps we take to protect our intellectual property rights may be inadequate. As of March 31, 2018, we have 12 patents issued and 12 patent applications pending in the United States. We also have 4 patents issued and 5 patent applications pending for examination in non-U.S. jurisdictions. We may not be able to obtain any further patents, and our

pending applications may not result in the issuance of patents. We have issued patents and pending patent applications outside the United States, and we may have to expend significant resources to obtain additional patents as we expand our international operations due to the cost of monitoring and protecting our rights across multiple jurisdictions.

In order to protect our intellectual property rights, we may be required to spend significant resources to monitor and protect these rights. Litigation brought to protect and enforce our intellectual property rights could be costly, time-consuming and distracting to management and could result in the impairment or loss of portions of our intellectual property. Failure to adequately enforce our intellectual property rights could also result in the impairment or loss of those rights. Furthermore, our efforts to enforce our intellectual property rights may be met with defenses, counterclaims and countersuits attacking the validity and enforceability of our intellectual property rights. Patent, copyright, trademark and trade secret laws offer us only limited protection and the laws of many of the countries in which we sell our services do not protect proprietary rights to the same extent as the United States and Europe. Accordingly, defense of our trademarks and proprietary technology may become an increasingly important issue as we continue to expand our operations and solution development into countries that provide a lower level of intellectual property protection than the United States or Europe. Policing unauthorized use of our intellectual property and technology is difficult and the steps we take may not prevent misappropriation of the intellectual property or technology on which we rely. For example, in the event of inadvertent or malicious disclosure of our proprietary technology, trade secret laws may no longer afford protection to our intellectual property rights in the areas not otherwise covered by patents or copyrights. Accordingly, we may not be able to prevent third parties from infringing upon or misappropriating our intellectual property. Our failure to secure, protect and enforce our intellectual property rights could materially adversely affect our brand and our business.

We may elect to initiate litigation in the future to enforce or protect our proprietary rights or to determine the validity and scope of the rights of others. That litigation may not be ultimately successful and could result in substantial costs to us, the reduction or loss in intellectual property protection for our technology, the diversion of our management’s attention and harm to our reputation, any of which could materially and adversely affect our business and results of operations.

We may be sued by third parties for alleged infringement of their proprietary rights.

There is considerable patent and other intellectual property development activity in our industry. Our success depends, in part, on our not infringing upon the intellectual property rights of others. Our competitors, as well as a number of other entities, including non-practicing entities, which are entities that have no operating business but exist purely as collectors of patents, and individuals, may own or claim to own intellectual property relating to our industry.

From time to time, certain third parties have claimed that we are infringing upon their intellectual property rights. In the future, we may be found to be infringing upon such rights. We closely monitor all such claims and none of the claims by the third parties have resulted in litigation, but legal actions by such parties are still possible. In addition, we cannot assure you that actions by other third parties alleging infringement by us of third-party patents or other intellectual property will not be asserted or prosecuted against us. In the future, others may claim that our services and underlying technology infringe or violate their intellectual property rights. We may also be unaware of the intellectual property rights that others may claim cover some or all of our technology or services. Any claims or litigation could cause us to incur significant expenses and, if successfully asserted against us, could require that we pay substantial damages or ongoing royalty payments, prevent us from offering our services, or require that we comply with other unfavorable terms. Under all of our sales contracts, we are obligated to indemnify our customers and channel partners against third-party infringement claims, and we may also be obligated to pay substantial settlement costs, including royalty payments, in connection with any such claim or litigation and to obtain licenses, modify services or refund fees, any of which could be costly. Even if we were to prevail in such a dispute, any litigation regarding intellectual property could be costly and time-consuming and divert the attention of our management and key personnel from our

business operations.

Confidentiality arrangements with employees and others may not adequately prevent disclosure of trade secrets and other proprietary information.

We have devoted substantial resources to the development of our technology, business operations and business plans. In order to protect our trade secrets and proprietary information, we rely in significant part on confidentiality arrangements with our employees, licensees, independent contractors, advisers, channel partners, resellers and customers. These arrangements may not be effective to prevent disclosure of confidential information, including trade secrets, and may not provide an adequate remedy in the event of unauthorized disclosure of confidential information. In addition, if others independently discover trade secrets and proprietary information, we would not be able to assert trade secret rights against such parties. Effective trade secret protection may not be available in every country in which our services are available or where we have employees or independent contractors. The loss of trade secret protection could make it easier for third parties to compete with our solutions by copying functionality. In addition, any changes in, or unexpected interpretations of, the trade secret and employment laws in any country in which we operate may compromise our ability to enforce our trade secret and intellectual property rights. Costly and time-consuming litigation could be necessary to enforce and determine the scope of our proprietary rights, and failure to obtain or maintain trade secret protection could adversely affect our competitive business position.

We may be subject to damages resulting from claims that our employees or contractors have wrongfully used or disclosed alleged trade secrets of their former employers or other parties.

We could in the future be subject to claims that employees or contractors, or we, have inadvertently or otherwise used or disclosed trade secrets or other proprietary information of our competitors or other parties. Litigation may be necessary to defend against these claims. If we fail in defending against such claims, a court could order us to pay substantial damages and prohibit us from using technologies or features that are essential to our solutions, if such technologies or features are found to incorporate or be derived from the trade secrets or other proprietary information of these parties. In addition, we may lose valuable intellectual property rights or personnel. A loss of key personnel or their work product could hamper or prevent our ability to develop, market and support potential solutions or enhancements, which could severely harm our business. Even if we are successful in defending against these claims, such litigation could result in substantial costs and be a distraction to management.

The use of open source software in our offerings may expose us to additional risks and harm our intellectual property.

Open source software is typically freely accessible, usable and modifiable. Certain open source software licenses require a user who intends to distribute the open source software as a component of the user's software to disclose publicly part or all of the source code to the user's software. In addition, certain open source software licenses require the user of such software to make any derivative works of the open source code available to others on unfavorable terms or at no cost. This can subject previously proprietary software to open source license terms.

We monitor and control our use of open source software in an effort to avoid unanticipated conditions or restrictions on our ability to successfully commercialize our products and solutions and believe that our compliance with the obligations under the various applicable licenses has mitigated the risks that we have triggered any such conditions or restrictions. However, such use may have inadvertently occurred in the development and offering of our products and solutions. Additionally, if a third-party software provider has incorporated certain types of open source software into software that we have licensed from such third-party, we could be subject to the obligations and requirements of the applicable open source software licenses. This could harm our intellectual property position and have a material adverse effect on our business, results of operations and financial condition.

The terms of many open source software licenses have not been interpreted by U.S. or foreign courts, and there is a risk that those licenses could be construed in a manner that imposes unanticipated conditions or restrictions on our ability to successfully commercialize our products and solutions. For example, certain open source software licenses may be interpreted to require that we offer our products or solutions that use the open source software for no cost; that we make available the source code for modifications or derivative works we create based upon, incorporating or using the open source software (or that we grant third parties the right to decompile, disassemble, reverse engineer, or otherwise derive such source code); that we license such modifications or derivative works under the terms of the particular open source license; or that otherwise impose limitations, restrictions or conditions on our ability to use, license, host, or distribute our products and solutions in a manner that limits our ability to successfully commercialize our products.

We could, therefore, be subject to claims alleging that we have not complied with the restrictions or limitations of the applicable open source software license terms or that our use of open source software infringes the intellectual property rights of a third-party. In that event, we could incur significant legal expenses, be subject to significant damages, be enjoined from further sale and distribution of our products or solutions that use the open source software, be required to pay a license fee, be forced to reengineer our products and solutions, or be required to comply with the foregoing conditions of the open source software licenses (including the release of the source code to our proprietary software), any of which could adversely affect our business. Even if these claims do not result in litigation or are resolved in our favor or without significant cash settlements, the time and resources necessary to resolve them could

harm our business, results of operations, financial condition and reputation.

Additionally, the use of open source software can lead to greater risks than the use of third-party commercial software, as open source software does not come with warranties or other contractual protections regarding indemnification, infringement claims or the quality of the code.

Risks Related to Ownership of Our Ordinary Shares and Our Organization in Jersey

Our share price has been and may continue to be volatile.

The market price of our ordinary shares may decline. In addition, the market price of our ordinary shares could be highly volatile and may fluctuate substantially as a result of many factors, many of which we cannot control, including:

- actual or anticipated fluctuations in our results of operations;
- variance in our financial performance from the expectations of market analysts;

- announcements by us or our competitors of significant business developments, changes in service provider relationships, acquisitions or expansion plans;
- changes in the prices of our services or those of our competitors;
- our involvement in litigation;
- our sale of ordinary shares or other securities in the future;
- market conditions in our industry;
- changes in key personnel;
- the trading volume of our ordinary shares;
- changes in the estimation of the future size and growth rate of our markets; and
- general economic and market conditions.

In addition, the stock markets have experienced extreme price and volume fluctuations. Broad market and industry factors may materially harm the market price of our ordinary shares, regardless of our operating performance. In the past, following periods of volatility in the market price of a company's securities, securities class action litigation has often been instituted against that company. If we were involved in any similar litigation we could incur substantial costs and our management's attention and resources could be diverted.

If securities or industry analysts cease to publish research or publish inaccurate or unfavorable research about our business, our share price and trading volume could decline.

The trading market for our ordinary shares depends in part on the research and reports that securities or industry analysts publish about us or our business. If one or more of the analysts who covers us downgrades our shares or publishes inaccurate or unfavorable research about our business, our share price would likely decline. If one or more of these analysts ceases coverage of us or fails to publish reports on us regularly, demand for our shares could decrease, which could cause our share price and trading volume to decline.

We do not expect to pay dividends and investors should not buy our ordinary shares expecting to receive dividends.

We do not anticipate that we will declare or pay any dividends in the foreseeable future, and our ability to do so may be constrained by restrictions in future debt arrangements, if any, and by Jersey law. Consequently, you will only realize an economic gain on your investment in our ordinary shares if the price appreciates. You should not purchase our ordinary shares expecting to receive cash dividends. Since we do not pay dividends, and if we are not successful in establishing an orderly trading market for our shares, then you may not have any manner to liquidate or receive any payment on your investment. Therefore, our failure to pay dividends may cause you to not see any return on your investment even if we are successful in our business operations. In addition, because we do not pay dividends we may have trouble raising additional funds which could affect our ability to expand our business operations.

The market price of our ordinary shares could be negatively affected by future sales of our ordinary shares.

Sales by us or our shareholders of a substantial number of ordinary shares in the public market, or the perception that these sales might occur, could cause the market price of our ordinary shares to decline or could impair our ability to raise capital through a future sale of, or pay for acquisitions using, our equity securities.

We have filed with the SEC a Registration Statement on Form F-3, commonly referred to as a "shelf registration," that permits us to sell in a registered offering up to $50 million of our securities at our discretion. The shelf registration was declared effective by the SEC in March 2017. While we have no current plans to conduct an offering of securities under the shelf registration statement, our plans could change at any time. In addition, the shelf registration statement also covers the registration of a significant number of ordinary shares held by our existing shareholders. By agreement, these shareholders are entitled to demand that we register their shares under the Securities Act of 1933, as amended, or the Securities Act, for resale into the public markets and they could exercise their rights by requiring that

we initiate an offering under the shelf registration statement.

In addition to our current shareholders' registration rights and our existing shelf registration statement, as of March 31, 2018, we had outstanding options and unvested restricted share units to purchase 6,262,623 shares under our equity incentive plans and had an additional 8,761,886 shares available for future grant.

As a result of the loss of our foreign private issuer status, we are now required to comply with the Exchange Act's domestic reporting regime, which will cause us to incur significant legal, accounting and other expenses.

As of September 30, 2017, we determined that we no longer qualify as a "foreign private issuer" as such term is defined in Rule 405 under the Securities Act, which means that we are required to comply with all of the periodic disclosure and current reporting requirements of the Exchange Act applicable to U.S. domestic issuers as of April 1, 2018. As of April 1, 2018, we have been required to comply with the Exchange Act reporting and other requirements applicable to U.S. domestic issuers, which are more detailed and extensive than the requirements for foreign private issuers. We have been required to make changes in our corporate governance practices in accordance with various SEC and NASDAQ rules. In addition, our officers and directors are no longer exempt from the reporting and "short-swing" profit recovery provisions of Section 16 of the Exchange Act and related rules with respect to their purchase and sales of our securities. As a result of such compliance, the regulatory and compliance costs to us under U.S. securities laws may be significantly higher than the cost we would incur as a foreign private issuer and therefore, we expect that the loss of foreign private issuer status will increase our legal and financial compliance costs and would make some activities highly time consuming and costly.

We must maintain proper and effective internal controls over financial reporting and any failure to maintain the adequacy of these internal controls may adversely affect investor confidence in our company and, as a result, the value of our ordinary shares.

We are required, pursuant to Section 404 of the Sarbanes-Oxley Act and the related rules adopted by the SEC, to furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting on an annual basis. This assessment includes disclosure of any material weaknesses identified by our management in our internal control over financial reporting. During the evaluation and testing process, if we identify one or more material weaknesses in our internal control over financial reporting, we will be unable to assert that our internal controls are effective.

In addition, our independent registered public accounting firm must attest to the effectiveness of our internal control over financial reporting under Section 404. Our independent registered public accounting firm may issue a report that is adverse in the event it is not satisfied with the level at which our controls are documented, designed or operating. We may not be able to remediate any future material weaknesses, or to complete our evaluation, testing and any required remediation in a timely fashion. We are also required to disclose significant changes made in our internal control procedures on a quarterly basis. Our compliance with Section 404 will require that we incur substantial accounting expense and expend significant management efforts.

Any failure to maintain internal control over financial reporting could severely inhibit our ability to accurately report our financial condition or results of operations. If we are unable to assert that our internal control over financial reporting is effective or our independent registered public accounting firm is unable to express an opinion on the effectiveness of our internal controls when it is required to issue such opinion, we could lose investor confidence in the accuracy and completeness of our financial reports, the market price of our ordinary shares could decline, and we could be subject to sanctions or investigations by NASDAQ, the SEC or other regulatory authorities.

Changes in U.S. tax laws could have a material adverse effect on our business, cash flow, results of operations or financial conditions.

The Tax Cuts and Jobs Act of 2017, which has been passed by the U.S. Congress and signed by the President, contains many significant changes to the U.S. federal income tax laws, the consequences of which have not yet been fully determined. Changes in corporate tax rates, the realizability of the net deferred tax assets relating to our U.S. subsidiary, and the deductibility of expenses contained in the Tax Cuts and Jobs Act or other tax reform legislation

could have a material impact on the value of our deferred tax assets, could result in significant one-time charges in the current or future taxable years, and could increase our future U.S. tax expense. The foregoing items could have a material adverse effect on our business, cash flow, results of operations or financial conditions.

A change in our tax residence could have a negative effect on our future profitability.

Although we are organized under the laws of the Bailiwick of Jersey, our affairs are, and are intended to continue to be, managed and controlled in the United Kingdom for tax purposes and therefore we are resident in the United Kingdom for U.K. and Jersey tax purposes. It is possible that in the future, whether as a result of a change in law or the practice of any relevant tax authority or as a result of any change in the conduct of our affairs or for any other reason, we could become, or be regarded as having become, a resident in a jurisdiction other than the United Kingdom. If we cease to be a U.K. tax resident, we may be subject to a charge to U.K. corporation tax on chargeable gains on our assets and to unexpected tax charges in other jurisdictions on our income. Similarly, if the tax residency of any of our subsidiaries were to change from their current jurisdiction for any of the reasons listed above, we may be subject to a charge to local capital gains tax on the assets.

Taxing authorities could reallocate our taxable income among our subsidiaries, which could increase our consolidated tax liability.

We conduct operations world-wide through subsidiaries in various tax jurisdictions pursuant to transfer pricing arrangements between our company and its subsidiaries. If two or more affiliated companies are located in different countries, the tax laws or regulations of each country generally will require that transfer prices be the same as those between unrelated companies dealing at arm's length and that appropriate documentation is maintained to support the transfer pricing. While we believe that we operate in compliance with applicable transfer pricing laws and intend to continue to do so, our transfer pricing procedures are not binding on applicable tax authorities. If tax authorities in any of these countries were to successfully challenge our transfer prices as not reflecting arms' length transactions, they could require us to adjust our transfer prices and thereby reallocate our income to reflect these revised transfer prices, which could result in a higher tax liability to us. In addition, if the country from which the income is reallocated does not agree with the reallocation, both countries could tax the same income, resulting in double taxation. If tax authorities were to allocate income to a higher tax jurisdiction, subject our income to double taxation or assess interest and penalties, it would increase our consolidated tax liability, which could adversely affect our financial condition, results of operations and cash flows. Double taxation should be mitigated in these circumstances where the affiliated parties that are subject to the transfer pricing adjustments are able to benefit from any applicable double taxation agreement.

Our ability to use our net operating loss carry forwards may be subject to limitation.

As of March 31, 2018, we had approximately $52.6 million, $56.4 million, $39.5 million, $17.3 million, and $2.4 million in U.K., U.S. federal, U.S. state, Australia, and Germany net operating losses, respectively. As of March 31, 2018, we also had a $1.2 million U.K. income tax credit carryforward. Each jurisdiction in which we operate may have its own limitations on our ability to utilize net operating losses or tax credit carryovers generated in that jurisdiction that may increase our U.K. and/or foreign income tax liability.

U.S. holders of our ordinary shares could be subject to material adverse tax consequences if we are considered a Passive Foreign Investment Company, or PFIC, for U.S. federal income tax purposes.

We do not believe that we were a PFIC for U.S. federal income tax purposes during the tax year ending March 31, 2018 and do not expect to be a PFIC for U.S. federal income tax purposes in the tax year. We also do not expect to become a PFIC in the foreseeable future, but the possible status as a PFIC must be determined annually and therefore may be subject to change. If we are at any time treated as a PFIC, such treatment could result in a reduction in the after-tax return to U.S. holders of our ordinary shares and may cause a reduction in the value of such shares. Furthermore, if we are at any time treated as a PFIC, U.S. holders of our ordinary shares could be subject to greater U.S. income tax liability than might otherwise apply, imposition of U.S. income tax in advance of when tax would otherwise apply and detailed tax filing requirements that would not otherwise apply. For U.S. federal income tax purposes, "U.S. holders" include individuals and various entities. A corporation is classified as a PFIC for any taxable year in which (i) at least 75% of its gross income is passive income or (ii) at least 50% of the average quarterly value of all its total gross assets is attributable to assets that produce or are held for the production of passive income. For this purpose, passive income includes certain dividends, interest, royalties and rents that are not derived in the active conduct of a trade or business. The PFIC rules are complex and a U.S. holder of our ordinary shares is urged to consult its own tax advisors regarding the possible application of the PFIC rules to it in its particular circumstances.

U.S. shareholders may not be able to enforce civil liabilities against us.

Several of our directors and executive officers are not residents of the United States, and all or a substantial portion of the assets of such persons are located outside the United States. As a result, it may not be possible for investors to

effect service of process within the United States upon such persons or to enforce against them judgments obtained in U.S. courts predicated upon the civil liability provisions of the federal securities laws of the United States.

There is also a doubt as to the enforceability in England and Wales and Jersey, whether by original actions or by seeking to enforce judgments of U.S. courts, of claims based on the federal securities laws of the United States. In addition, punitive damages in actions brought in the United States or elsewhere may be unenforceable in England and Wales and Jersey.

The rights afforded to shareholders are governed by Jersey law. Not all rights available to shareholders under English law or U.S. law will be available to shareholders.

The rights afforded to shareholders will be governed by Jersey law and by our Articles of Association, and these rights differ in certain respects from the rights of shareholders in typical English companies and U.S. corporations. In particular, Jersey law significantly limits the circumstances under which shareholders of companies may bring derivative actions and, in most cases, only the corporation may be the proper claimant or plaintiff for the purposes of maintaining proceedings in respect of any wrongful act committed against it. Neither an individual nor any group of shareholders has any right of action in such circumstances. In addition, Jersey law does not afford appraisal rights to dissenting shareholders in the form typically available to shareholders of a U.S. corporation.

Item 1B. Unresolved Staff Comments.

None.

Item 2. Properties.

Principal Office Locations

The table below describes our existing principal office facilities, all of which are leased, or, in the case of our new U.K. Global Headquarters, is under an agreement for lease.

| Location | Purpose | Square Footage | Expiration |
|---|---|---|---|
| London, United Kingdom | Global Headquarters | 57,093 | 12/1/2019 |
| London, United Kingdom | Global Headquarters (projected December 2019) | 112,888 | 1/1/2029 |
| Lexington, Massachusetts USA | North American Headquarters | 79,145 | 1/31/2028 |
| Watertown, Massachusetts USA | Former North American Headquarters | 44,170 | 10/31/2020 |
| Johannesburg, South Africa | South African Headquarters | 22,722 | 9/30/2018 |

We maintain additional leased office facilities in Cape Town, South Africa, Melbourne and Sydney, Australia, Munich, Germany, Amsterdam, the Netherlands, Dubai, UAE, as well as in Chicago, Dallas and San Francisco in the United States.

We believe that the total space available to us in the facilities under our current leases or an agreement for lease, or obtainable by us on commercially reasonable terms, will meet our needs for the foreseeable future.

Data Centers

We have two data centers in each of the United States, the United Kingdom, South Africa, Australia, Jersey, Channel Islands and Germany. Our data center leases expire between 2020 and 2023. We have capacity headroom built into our primary data center leases to accommodate infrastructure growth within the lease periods should we need to add more space or power to our existing footprint.

For more information about our lease and data center commitments, see also Note 12, Commitments and Contingencies, of the Notes to our Consolidated Financial Statements, included elsewhere in this Annual Report on Form 10-K.

Item 3. Legal Proceedings.

From time to time, we may be involved in legal proceedings and subject to claims in the ordinary course of business. Although the results of these proceedings and claims cannot be predicted with certainty, we do not believe the ultimate cost to resolve these matters would individually, or taken together, have a material adverse effect on our business, operating results, cash flows or financial condition. Regardless of the outcome, such proceedings can have an adverse impact on us because of defense and settlement costs, diversion of resources and other factors, and there can be no assurances that favorable outcomes will be obtained.

Item 4. Mine Safety Disclosures.

Not applicable.

PART II

Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities.

Market Information

Our ordinary shares are listed on The Nasdaq Global Select Market under the symbol "MIME."

The following table sets forth the reported high and low sales prices of our ordinary shares for the periods indicated, as quoted on the Nasdaq Global Select Market:

| Year Ended March 31, 2018 | High | Low |
|---|---|---|
| First Quarter | $29.48 | $20.91 |
| Second Quarter | $30.10 | $25.12 |
| Third Quarter | $32.00 | $26.50 |
| Fourth Quarter | $39.33 | $28.14 |
| Year Ended March 31, 2017 | | |
| First Quarter | $12.15 | $7.08 |
| Second Quarter | $20.10 | $9.50 |
| Third Quarter | $24.60 | $17.35 |
| Fourth Quarter | $23.10 | $16.75 |

Shareholders

As of March 31, 2018, there were 93 holders of record of our ordinary shares, including Cede & Co., a nominee for The Depository Trust Company, or DTC, which holds shares of our ordinary shares on behalf of an indeterminate number of beneficial owners. All of the ordinary shares held by brokerage firms, banks and other financial institutions as nominees for beneficial owners are deposited into participant accounts at DTC, and are considered to be held of record by Cede & Co. as one shareholder. Because many of our shares are held by brokers and other institutions on behalf of shareholders, we are unable to estimate the total number of shareholders represented by these record holders.

Dividends

We have never declared or paid, and do not anticipate declaring or paying in the foreseeable future, any cash dividends on our ordinary shares. Any future determination as to the declaration and payment of dividends, if any, will be at the discretion of our board of directors, subject to applicable laws, including the laws of the Bailiwick of Jersey, and will depend on then existing conditions, including our financial condition, operating results, contractual restrictions, capital requirements, business prospects and other factors our board of directors may deem relevant.

Recent Sales of Unregistered Securities

None.

Use of Proceeds from Initial Public Offering of Ordinary Shares

Our initial public offering of ordinary shares was effected through the filing of a Registration Statement on Form F-1 (File No. 333-207454), which was declared effective by the SEC on November 18, 2015. There has been no material change in the use of proceeds from our initial public offering as described in our final prospectus filed with the SEC pursuant to Rule 424(b).

Purchase of Equity Securities by the Issuer and Affiliated Purchasers

None.

Securities Authorized for Issuance Under Equity Compensation Plans

Information about securities authorized for issuance under our equity compensation plan is incorporated herein by reference to Item 12 of Part III of this Annual Report on Form 10-K.

Stock Performance Graph

The graph below compares the cumulative total return to shareholders on our ordinary shares for the period from November 19, 2015 (the first date that our ordinary shares were publicly traded) through March 31, 2018 against the cumulative total return of the Russell 2000 Index and the NASDAQ Computer Index. The comparison assumes $100 was invested in our ordinary shares and each of the indices and the reinvestment of dividends, if any.

The performance shown on the graph below is based on historical results and is not indicative of, nor intended to forecast, future performance of our ordinary shares.

| | 11/19/15 | 3/31/16 | 3/31/17 | 3/31//18 |
|---|---|---|---|---|
| Mimecast Limited | 100.00 | 96.34 | 221.68 | 350.79 |
| Russell 2000 Index | 100.00 | 96.58 | 121.90 | 136.28 |
| NASDAQ Computer Index | 100.00 | 100.25 | 127.61 | 162.86 |

This performance graph and related information shall not be deemed to be “soliciting material” or “filed” for purposes of Section 18 of the Exchange Act, nor shall such information be incorporated by reference into any filing of Mimecast Limited under the Exchange Act or the Securities Act, except to the extent that we specifically incorporate it by reference in such filing.

Item 6. Selected Financial Data.

Our historical consolidated financial statements are prepared in accordance with U.S. GAAP and presented in U.S. dollars. The selected historical consolidated financial information set forth below has been derived from our historical consolidated financial statements for the years presented. Historical information as of March 31, 2018 and 2017 and for the years ended March 31, 2018, 2017 and 2016 is derived from our audited consolidated financial statements included elsewhere in this Annual Report on Form 10-K. Historical financial information as of March 31, 2016, 2015 and 2014 and for the years ended March 31, 2015 and 2014 is derived from our audited consolidated financial statements not included in this Annual Report on Form 10-K. You should read the information presented below in conjunction with Item 7, “Management’s Discussion and Analysis of Financial Condition and Results of Operations,” and our consolidated financial statements and the related notes appearing in Item 8. “Financial Statements and Supplementary Data,” of this Annual Report on Form 10-K to fully understand the factors that may affect the comparability of the information presented below.

The selected consolidated financial data in this section are not intended to replace the consolidated financial statements and are qualified in their entirety by the consolidated financial statements and related notes included elsewhere in this Annual Report on Form 10-K.

| | Year Ended March 31, | | | | |
|---|---|---|---|---|---|
| | 2018 | 2017 | 2016 | 2015 | 2014 |
| | (in thousands, except per share data) | | | | |
| Consolidated Statements of Operations Data: | | | | | |
| Revenue | $261,897 | $186,563 | $141,841 | $116,085 | $88,315 |
| Cost of revenue (1) | 69,699 | 50,314 | 41,809 | 36,821 | 28,673 |
| Gross profit | 192,198 | 136,249 | 100,032 | 79,264 | 59,642 |
| Operating expenses | | | | | |
| Research and development (1) | 38,373 | 22,593 | 17,663 | 14,461 | 12,844 |
| Sales and marketing (1) | 121,246 | 96,154 | 65,187 | 51,224 | 46,971 |
| General and administrative (1) | 36,989 | 27,875 | 19,756 | 15,806 | 11,187 |
| Impairment of long-lived assets | 1,712 | — | — | — | — |
| Restructuring | 832 | — | — | 1,203 | — |
| Total operating expenses | 199,152 | 146,622 | 102,606 | 82,694 | 71,002 |
| Loss from operations | (6,954) | (10,373) | (2,574) | (3,430) | (11,360) |
| Other income (expense) | | | | | |
| Interest income | 1,310 | 510 | 74 | 62 | 86 |
| Interest expense | (598) | (268) | (690) | (703) | (542) |
| Foreign exchange (expense) income | (3,511) | 6,892 | 811 | 4,508 | (5,055) |
| Other income, net | 72 | — | — | — | — |
| Total other income (expense), net | (2,727) | 7,134 | 195 | 3,867 | (5,511) |
| (Loss) income before income taxes | (9,681) | (3,239) | (2,379) | 437 | (16,871) |
| Provision for income taxes | 2,705 | 2,202 | 865 | 152 | 19 |
| Net (loss) income | $(12,386) | $(5,441) | $(3,244) | $285 | $(16,890) |
| Net (loss) income per share applicable to ordinary shareholders: (2) | | | | | |
| Basic | $(0.22) | $(0.10) | $(0.08) | $0.01 | $(0.53) |
| Diluted | $(0.22) | $(0.10) | $(0.08) | $0.01 | $(0.53) |
| Weighted-average number of ordinary shares used in computing net (loss) income per share applicable to ordinary shareholders: | | | | | |
| Basic | 57,269 | 54,810 | 40,826 | 32,354 | 31,719 |
| Diluted | 57,269 | 54,810 | 40,826 | 36,075 | 31,719 |

| | As of March 31, | | | | |
|---|---|---|---|---|---|
| | 2018 | 2017 | 2016 | 2015 | 2014 |
| | (in thousands) | | | | |
| Consolidated Balance Sheet Data: | | | | | |
| Cash, cash equivalents and investments | $137,210 | $111,666 | $106,140 | $32,890 | $19,158 |

| | | | | | |
|---|---|---|---|---|---|
| Property and equipment, net | 123,822 | 32,009 | 24,806 | 23,159 | 24,974 |
| Total assets | 358,398 | 205,352 | 175,127 | 88,829 | 75,783 |
| Debt and capital lease obligations, current and long-term | 3,515 | 2,203 | 6,891 | 12,364 | 9,092 |
| Deferred revenue, current and long-term | 141,102 | | | | |