Barracuda

QPCSS LTD. QUEENS PARK CyberSecurity Solutions Ltd.

Office 365 Adoption Survey

Drivers, Risks, and Opportunities

White Paper

Executive Summary

This survey was conducted by Barracuda in April 2017 with customers in North America, Europe, the Middle East, and Africa. It was designed to measure trends around the adoption and use of Microsoft Office 365 (Office 365), including factors contributing to their decisions to migrate, or in some cases, to stick with their existing platforms. It also gathered information about customers' use of third-party security and data protection solutions with Office 365, and about their engagement with VARs and MSPs.

Findings

Since the 2016 survey, adoption of Office 365 was found to have increased by more than 50 percent, indicating robust growth. There was also sizable growth in the percentage of customers reporting concerns with the native security, archiving, and backup features, validating the need for third-party solutions to augment native features.

The results also indicate very high concerns about ransomware in particular, along with notable worries about other advanced threats, including phishing and spear phishing. Large percentages also reported the opinion that the native security within Office 365 does not, by itself, offer sufficient protection against these threats.

Analysis

The availability of advanced, cloud-optimized solutions for securing, archiving, and backing up data in SaaS and cloud environments is helping to enable ongoing growth in the adoption of Office 365, breaking down security concerns.

Adoption is likely to accelerate as more buyers learn to plan for third-party security as a matter of course, just as they do for on-premises deployments. Many buyers understand the shared responsibility model of security as it applies to Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform. It may be that fewer have learned yet how it applies to Office 365.

Background

As Office 365 continues to grow subscriptions at record pace, Barracuda wanted to understand:

- What percentage of customers have already adopted Office 365
- Customer perception of Office 365 and the native features it offers
- The overall efficacy of native security, archiving, and data protection features
- Adoption rate of third-party solutions to augment native features
- Use of VAR or other partners

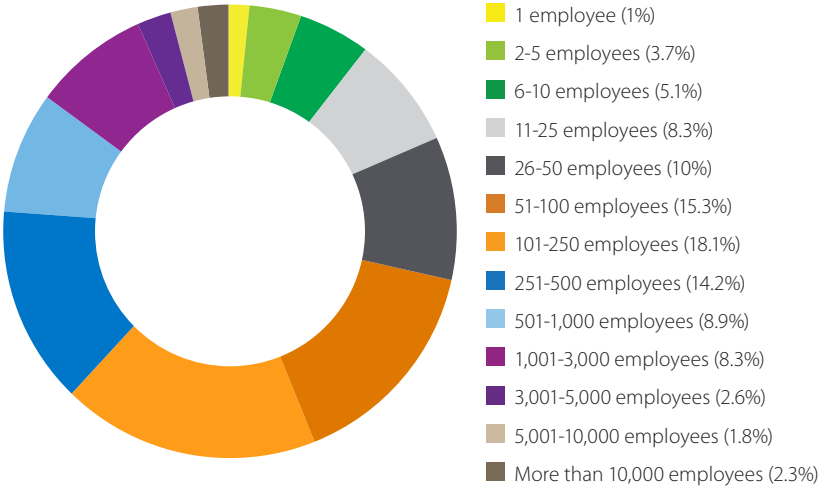
The transition from the traditional Microsoft Office suite to Office 365 is nearly transparent to end-users. However, in the aggregate it is a monumental shift of workloads, resources, and processes, and it has a profound impact on security, compliance, backup and recovery, and more.

Barracuda has been protecting Microsoft environments for nearly 15 years, and is a leader in security and data protection solutions for hybrid and cloud-based environments, partly thanks to its relentless focus on customer needs. By gathering and analyzing customer responses to this survey, Barracuda is able to refine and extend its vision of what's coming next, and to gain insights about how to best serve its customers' needs and preferences.

Survey Respondent Profile

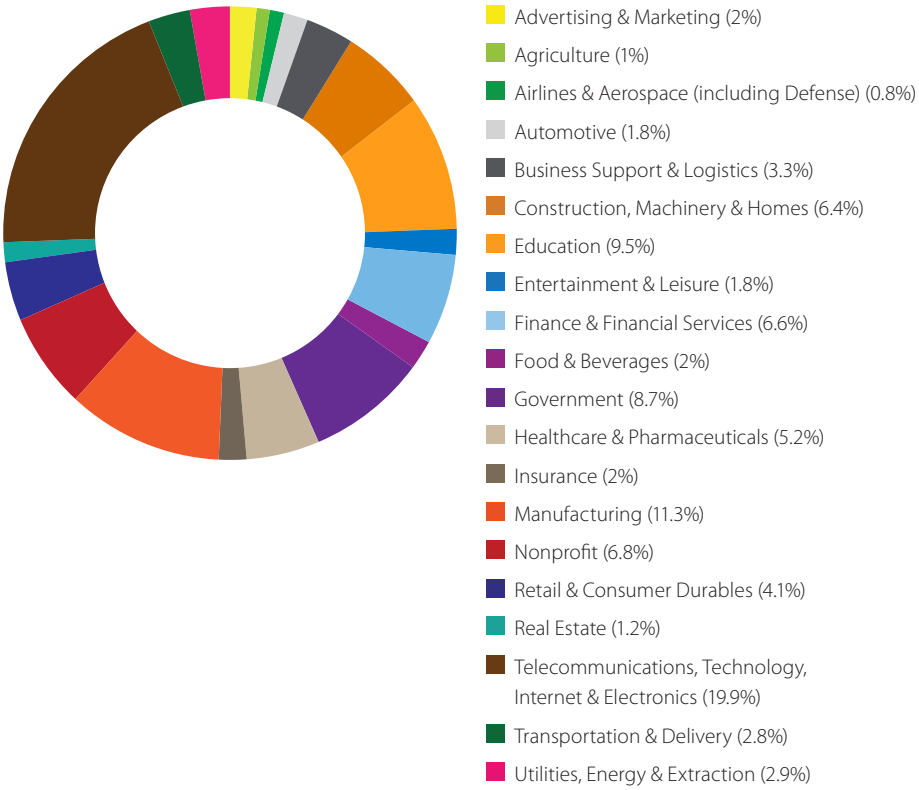
More than 1,000 organizations responded to the survey, ranging from very small to very large.

About how many employees work at your company?



Respondents represented a wide range of industries, with concentrations in Telecom/IT, Manufacturing, and Education.

Which of the following best describes the principal industry of your organization?

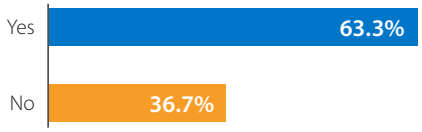


Survey Findings

Adoption Rates

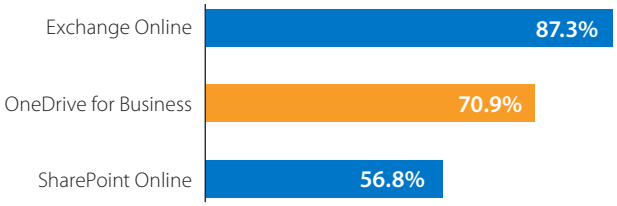
The overall percentage of respondents currently using Office 365 was 63.3 percent. This represents a significant increase over the 42 percent adoption rate reported in a similar survey conducted in 2016.

Are you currently using Office 365?



Exchange Online is the most commonly used feature of Office 365, however large numbers are also using OneDrive for Business and SharePoint Online.

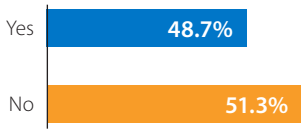
Which Office 365 features are you using?



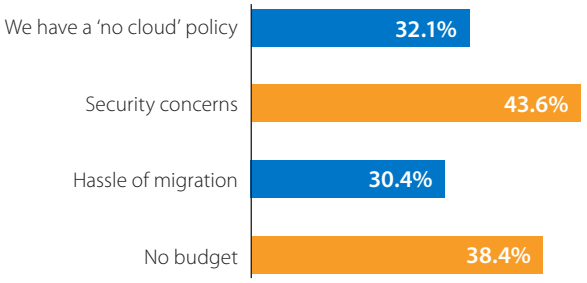
Intention to Adopt

Of the survey's respondents who have not yet migrated to Office 365, just under 50 percent reported that they were planning to do so. Among those reporting that they did not intend to adopt it, more than 32 percent cited a corporate "no-cloud" policy as the reason.

Are you planning to migrate to Office 365?



What are the reasons for not migrating?

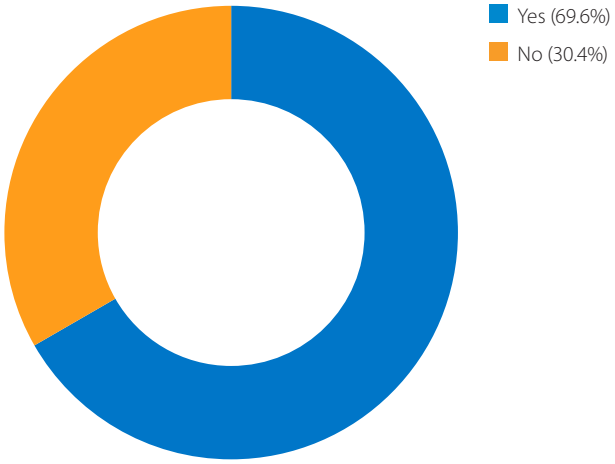


Security Concerns

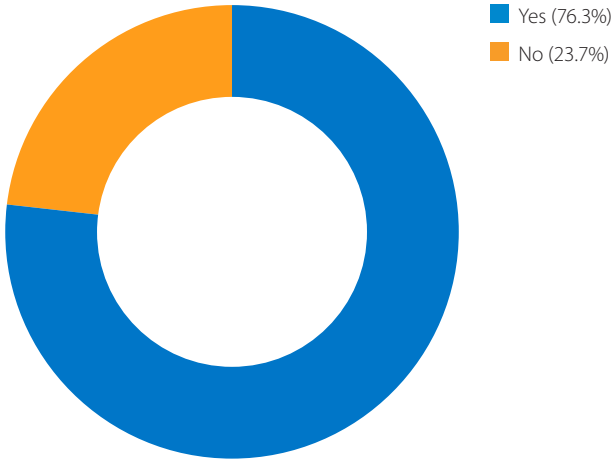
In the 2016 customer survey, the "no cloud" policy was by far the most cited reason for not migrating, with security concerns coming in at second place. In the new survey, security concerns took the top spot, at more than 43 percent.

Of those who had already migrated, nearly 70 percent reported significant concerns about advanced threats in their Office 365 environments. Among those planning to migrate, the number was 76.3 percent.

Are you concerned about advanced threats in your Office 365 environment?

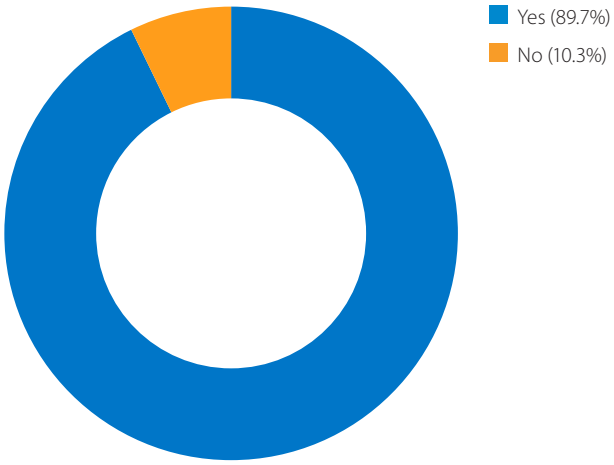


Are you concerned about advanced threats in your future Office 365 environment?



In addition, a very high number of respondents, nearly 90 percent, said they were concerned about latent malware in emails.

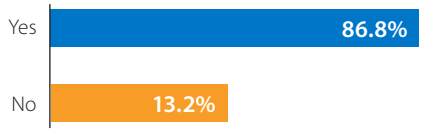
Are you concerned about latent malware in emails?



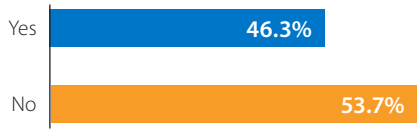
Phishing, Spear Phishing, and Social Engineering

Spear phishing is rapidly becoming the most significant security threat today. Nearly 89 percent of respondents reported that they are concerned about phishing, spear phishing, and social engineering, and just over 46 percent reported having been targeted by such attacks.

Are you concerned about phishing, spear phishing, impersonation, or social engineering attacks?

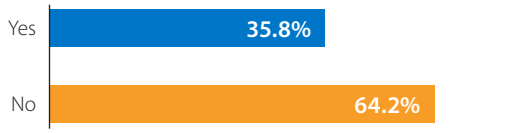


Has your organisation been the target of spear phishing, impersonation, or social engineering attacks?

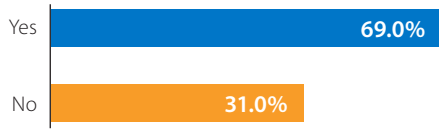


Despite high levels of concern, less than 36 percent of respondents said that they use a third-party solution to help mitigate threats from phishing, spear phishing, and social engineering. 69 percent reported that they train employees on how to recognize and avoid these types of threats, but only a little more than 19 percent use a third party to conduct this training.

Do you have an existing third-party solution for mitigating spear phishing, impersonation, or social engineering attacks?



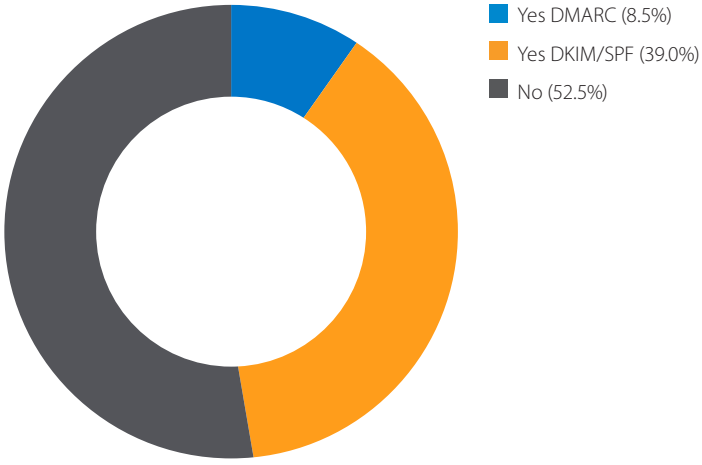
Do you currently train your employees on phishing and spear phishing prevention?



Do you have a third-party phishing and spear phishing training provider?

DMARC (Domain-based Message Authentication, Reporting & Conformance) and DKIM/SPF (DomainKeys Identified Mail/Sender Policy Framework) are standards-based protocols that can be helpful in reducing the threat from phishing, spear phishing, and social engineering. However, the number of respondents who have implemented either of them was considerably lower than those reporting high levels of concern, with 8.5 percent using DMARC and another 39 percent using DKIM/SPF.

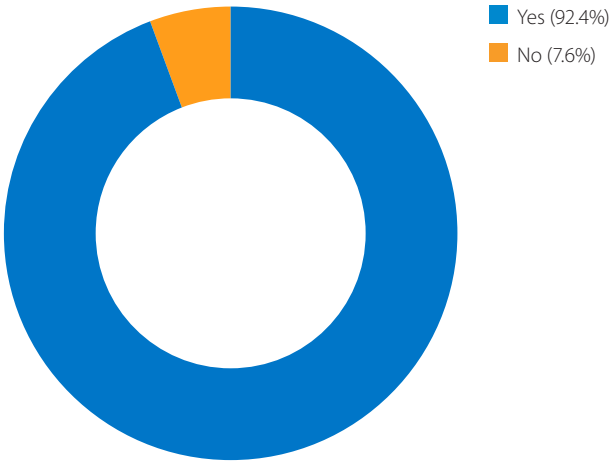
Have you set up DMARC or DKIM/SPF in your email environment?



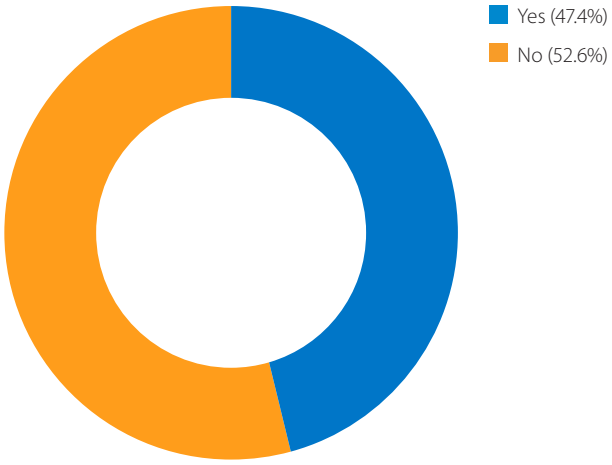
Ransomware

Ransomware is currently the most common and most successful form of advanced threat, and customers are aware of it. More than 92 percent of respondents said that ransomware is a concern, with more than 47 percent reporting that they had been a victim of ransomware. Of those who were able to identify the source of the ransomware attack, nearly 76 percent reported that it came via email—including phishing and spear-phishing emails.

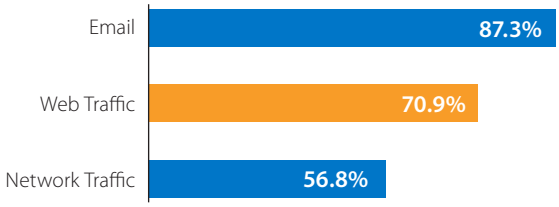
Is ransomware a concern for you and your organization?



Have you been a victim of ransomware?



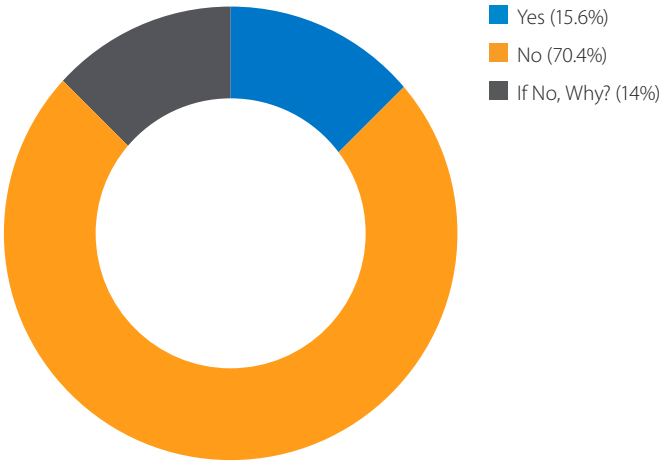
If yes, did the attack come through email, web traffic, network traffic?



Microsoft ATP

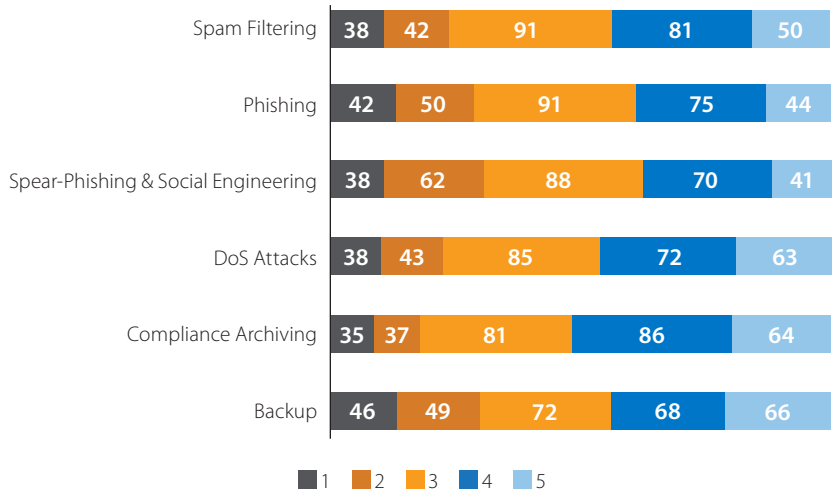
Microsoft offers an email security subscription service called Office 365 Advanced Threat Protection (ATP). The Barracuda survey revealed that a low number of customers using Office 365 have an added Microsoft ATP subscription, with more than 70 percent of respondents saying they were not using it.

Are you currently using Microsoft ATP?



Overall, respondents reported significant doubts about the effectiveness of native security and other features of Office 365. In particular, they had concerns about these features' ability to protect them effectively against ransomware, phishing, and spear-phishing or social-engineering attacks.

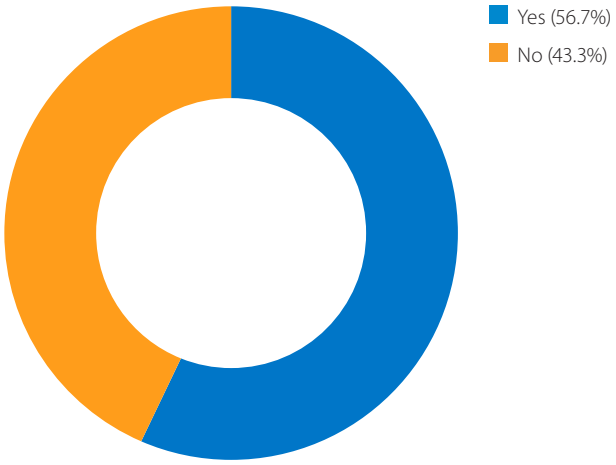
On a scale of 1-5, how do you think Office 365 features will meet your company's needs? (5 being fully)



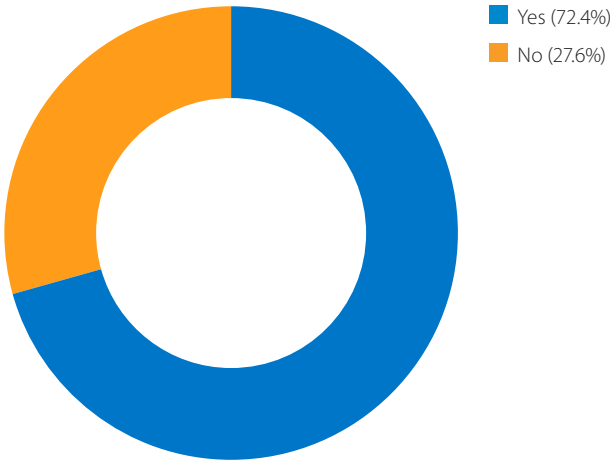
Third-Party Security

Nearly 57 percent of respondents said that they were augmenting their Office 365 deployments with third-party security, archiving, or backup solutions. Among those intending to migrate, the number was considerably higher, at more than 72 percent.

Are you using any third-party security, archiving, or backup solutions to augment your Office 365 protection?



Are you planning to use any third-party security, archiving, or backup solutions to augment your Office 365 protection?



VAR/MSP

More than 51 percent reported that they did use a VAR or service provider to manage the adoption, migration, and operation of their Office 365 deployment. Again, a higher number of respondents who were still intending to migrate—more than 60 percent—said they are planning to do so.

Did you consult with a Value Added Reseller (VAR) or Service Provider to manage the adoption, migration, and operation of Office 365 for you?

Will you consult with a Value Added Reseller (VAR) or Service Provider to manage the adoption, migration, and operation of Office 365 for you?

Like the findings about use of third-party solutions, these results reflect the growing awareness of the importance of effective security, and of the need for more than just the native security measures. It may also reflect the growing perception of migration to Office 365 as a hassle.

Analysis

No Industry-specific Trends

Although the survey sample included respondents across many industries and market sectors, as well as organizations ranging in size from one to more than 10,000 employees, the trends identified in the survey results were fairly evenly spread across industries and across sizes.

In part, these results reflect the fact that Microsoft Office has enjoyed near-universal use among organizations of all types, and that all users are currently being offered the same encouragements to migrate to Office 365. However, it also indicates that reasons for postponing or rejecting the move to Office 365—security concerns, lack of budget, and perceived hassle—are influencing very different types of organizations to roughly equal degrees.

Adoption Rates

Adoption of cloud platforms overall is growing rapidly. Whether it's AWS, Azure, Google Cloud Portal, Office 365, or other more specialized cloud environments, there is a clear overall trend in the direction of near-universal participation. In light of this, the 50 percent increase in Office 365 adoption over the previous year in our survey pool is consistent with expectations.

However, it is worth noting that in the preceding year's survey (2015-16), Office 365 subscriptions were reported to have doubled, whereas for this year (2016-17), within the survey sample, the increase was close to 50 percent—which means that the actual adoption rate has declined compared to last year.

This decline is undoubtedly partly due to the fact that early adopters move quickly as a group, while those who are more reluctant to adopt new technologies require differing periods of time to overcome their reluctance. Nonetheless, trends around the factors impeding adoption make it likely that with the right support from third parties, adoption rates could be accelerated significantly.

Factors Impeding Adoption

Security concerns were the top factor impeding adoption, followed by budget shortfalls and the perceived hassle of the transition. It's clear that there is room to accelerate adoption by addressing these factors and eliminating them.

Lack of budget to cover the up-front costs of adoption—data migration, training, infrastructure—was cited by 38.4 percent of respondents. This may reflect a lack of top-level buy-in for cloud projects, or a more general constriction of IT budgets. We can expect this factor to decline in importance as awareness of the realities of migration becomes more widespread.

It is notable that more than 30 percent of respondents reported that the hassle of migration is a decisive factor. In the 2016 EMEA survey, only 13 percent reported the same thing. Despite the fact that Microsoft has worked diligently to automate and simplify migration, the perception of it as a hassle appears to be growing.

However, this increase may actually be reflective of a positive trend overall. It seems likely that a growing number of customers are becoming aware that there is more to ensuring a secure, compliant, easy-to-manage deployment than simply switching to Office 365. The understanding that they must also attend to their share of responsibility for security, archiving, and ensuring compliance—just as with their on-premises Exchange deployments—may be contributing to a heightened perception of migration as a hassle.

As customers become more accustomed to the need to plan for security as a part of any cloud migration, this factor—along with the failure to budget appropriately—should decrease in significance.

Security and Ransomware

The very high rates of concern about security—including worries about latent threats, advanced malware, phishing and spear phishing, and especially ransomware—may be the single most important contributing factor to the overall decline in the rate of adoption that the survey revealed.

Ransomware—a type of malware that encrypts victims' data and files, with attackers demanding a ransom payment in exchange for the decryption key—is very fast-growing and successful. US businesses are estimated to have paid more than $200 million in ransom in 2016, with the 2017

total projected to exceed one billion dollars.

With numerous high-profile attacks being reported in the media, it is not surprising that growing numbers of customers are aware of, and concerned about, the very real ransomware threat.

In addition, a very high number of respondents, nearly 90 percent, said they were concerned about latent malware in emails. Most inboxes and other email stores include large numbers of emails containing malicious links or attachments. These latent threats are essentially dormant, but only until someone unwisely clicks on the wrong link or file.

It is strongly recommended that organizations of all sizes use a scanning tool to find and remove these threats either before or after migrating to Office 365, in order to begin a new security regime without threats already residing in their systems.

Engagement with Third-Party Providers, VARs, and MSPs

Growing rates of engagement with VARs and service providers, along with growing usage of third-party security and other solutions, indicate that the high ranking of security concerns is helping to drive more security-focused deployments. Clearly a growing number of customers are becoming aware of third-party options, and are seeking out professional guidance.

The higher percentage among those still planning to migrate is consistent with increasing awareness of security threats. It also illustrates growing understanding of the limitations of native security, and of how the shared-responsibility model for cloud security applies to data and workloads in Office 365.

Clearly this presents a market opportunity for VARs and managed service providers (MSP). Winners will be those who can provide services and solutions that make it simple to fully secure, archive, and back up both cloud-hosted and on-premises environments, and to make the transition to Office 365—and the integration of other cloud services and platforms—as easy and seamless as possible.

Conclusion

Adoption rates of Office 365 by Barracuda customers went up. At the same time, concerns about security (among other things) as a reason not to adopt it also went up quite a lot.

These apparently contradictory findings are reconciled by the further findings that the use of third-party security solutions, and of VARs or service providers, is also high and growing.

Barracuda Essentials is one of the industry's leading solutions to protect against email-borne attacks, spam, and viruses on Office 365. It addresses customers' security concerns with advanced features including attachment sandboxing, antivirus, anti-phishing, and typosquatting protection to secure against advanced threats, including new and unknown threats. Data loss protection and email encryption keep sensitive data such as credit cards and customer data safe. Secure archiving and backup helps customers ensure regulatory compliance.

Barracuda Sentinel is a cloud service that uses artificial intelligence (AI) to stop spear phishing and cyber fraud in real time. The service combines three powerful layers of artificial intelligence, domain fraud visibility, and protection using DMARC authentication. It also provides fraud simulation training for high-risk individuals inside an organization. It integrates directly with Office 365 via API, so there is no impact on network performance or user experience, and setup

typically takes less than five minutes. Barracuda Sentinel works alongside any existing email security solution, including Barracuda Essentials, native Office 365, and others.

Barracuda Essentials and Barracuda Sentinel are also ideally suited for managed service providers (MSP), with their pure-cloud architecture, easy-to-use centralized management, and support for multi-tenancy. The opportunities in this market are clearly on the rise, and Barracuda is well known as a supportive partner for MSPs, VARs, and customers.

About Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide, and are delivered in appliance, virtual appliance, cloud, and hybrid configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network security and data protection. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com