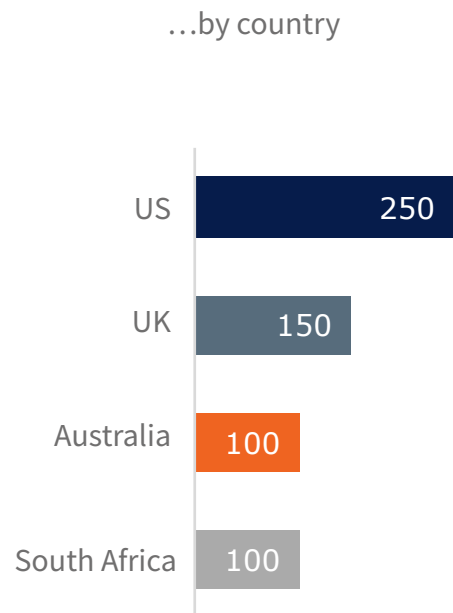# OFFICE 365
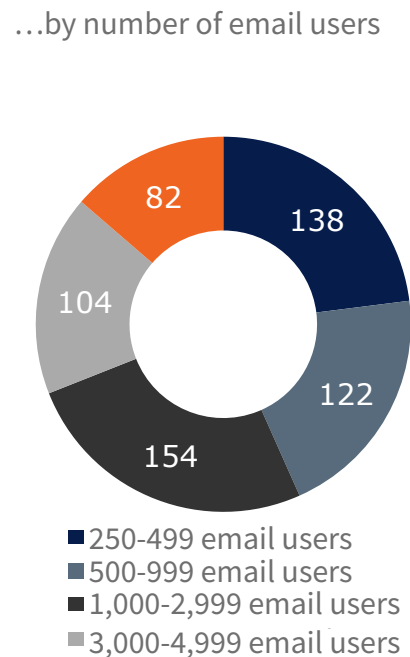# EXCHANGE ONLINE

Research Results
December 2016

mimecast®

Demographics

600 IT and business decision makers were interviewed in October/November 2016, split in the following ways…

…by country

US 250
UK 150
Australia 100
South Africa 100

Figure D1: Analysis of respondent country, asked to all 600 respondents

…by number of email users

82
138
122
154
104

- 250-499 email users
- 500-999 email users
- 1,000-2,999 email users
- 3,000-4,999 email users

Figure D2: "How many individual email users does your organization have globally?", *asked to all 600 respondents*

…by sector

Construction and property 53
IT, technology and telecoms 52
Business and professional services 51
Consumer services 51
Private healthcare 51
Energy, oil/gas and utilities 50
Financial services 50
Manufacturing and production 50
Media, leisure and entertainment 41
Local government 36
Private education 23
Public education 20
Public healthcare 17
Other sector 1

Figure D3: "Within which sector is your organization?", *asked to all 600 respondents*

research conducted by

VansonBourne
Intelligent Market Research

Four Areas of Interest:

Email Services

Email is undergoing a fundamental shift as organizations transition from on-premises to the cloud. See adoption rates, what percent of the total users are being moved to the cloud and the other Office 365 services that are being deployed.

Migration to Office 365

Moving to the cloud isn't as simple as clicking your heels together three times. Organizations need to plan what data to migrate and select a migration strategy to compliment their business.

Threat Protection

The threats to email don't change when moving to the cloud. In fact, the cloud introduces new risks that need to be mitigated along with the standard threats to email like spam, malware, spear-phishing, ransomware and impersonation attacks.
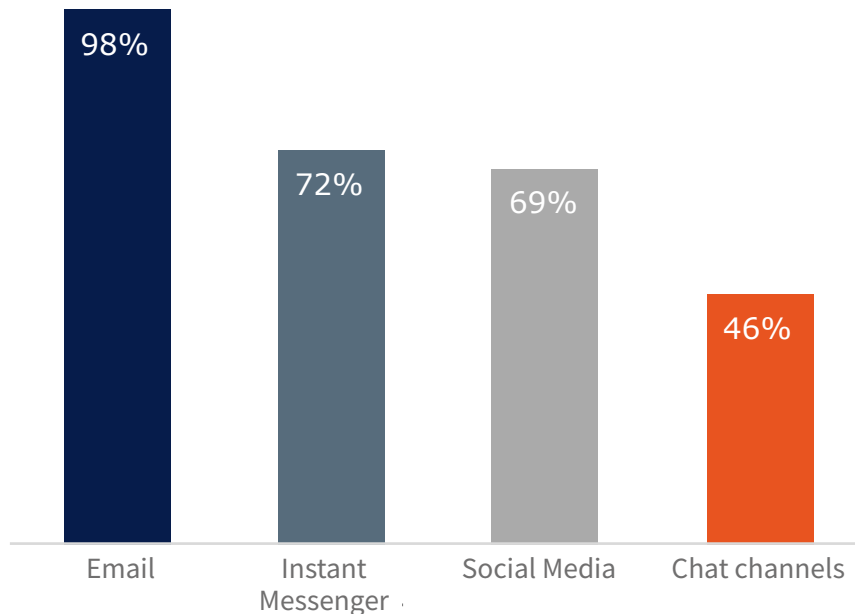
Email Challenges with Providers

Email remains the dominant form of business communication and productivity suffers when it doesn't work as expected. Learn just how critical it is and how organizations plan to keep email up and running in the cloud.

1: Email services

Online communication tools

The majority of respondents' organizations use multiple online communication tools.

Email (98%) is the most common. Around seven in ten use instant messenger (72%) and social media (69%). Just under half (46%) use chat channels.

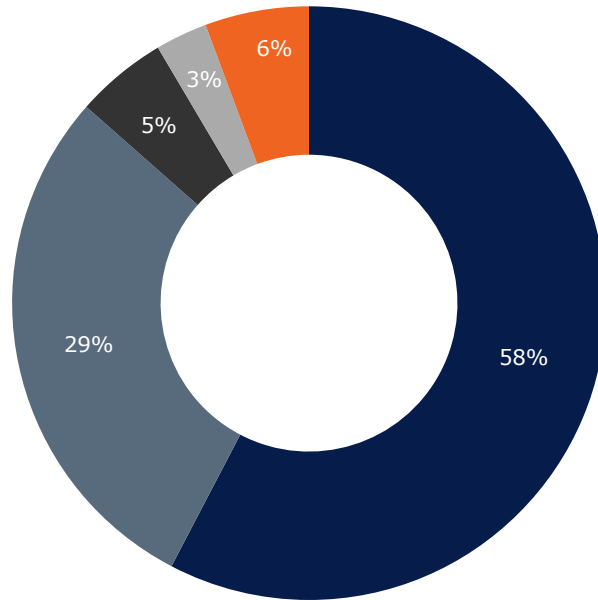This highlights that although most organizations have expanded into using more than one type of online communication tool, email remains the one that is being used by almost all.

So, are many respondents' organizations using Office 365 Exchange Online as their email provider?

Figure 1: "Which of the following online communication tools does your organization use?", *asked to all 600 respondents*

Adoption of Office 365 Exchange Online

Legend:
- ■ Yes, we are currently using it
- ■ Yes, we are planning to use it within the next 12 months
- ■ Yes, we are planning to use it within the next 12-24 months
- ■ Yes, we are planning to use it but not within the next 24 months
- ■ No, we have no plans to use it

Figure 2: "Is your organization already using, or planning to use Office 365 Exchange Online?", *asked to all 600 respondents*

The use of Exchange Online is driving adoption.

Around six in ten (58%) respondents' organizations are currently using Office 365 Exchange Online, while the vast majority (94%) are either currently using or planning to use it (figure 2).

Most organizations have an interest in using Office 365 Exchange Online, so what level of adoption do they anticipate?

Proportion of email users on Office 365 Exchange Online

Of those that have already adopted it, on average around 70% of total email users in respondents' organizations are using Office 365 Exchange Online currently (figure 3). Among respondents' organizations that plan to adopt it, the same proportion (70%) are anticipated to use Office 365 Exchange Online, on average (figure 4).

Most employees in organizations where Office 365 Exchange Online is used are actually making use of it, and in organizations that are planning to, the same can be said. But what other email providers are being used?

Legend:
- Fewer than 10%
- 10-30%
- 30-50%
- 50-70%
- 70-90%
- 90-99%
- 100%
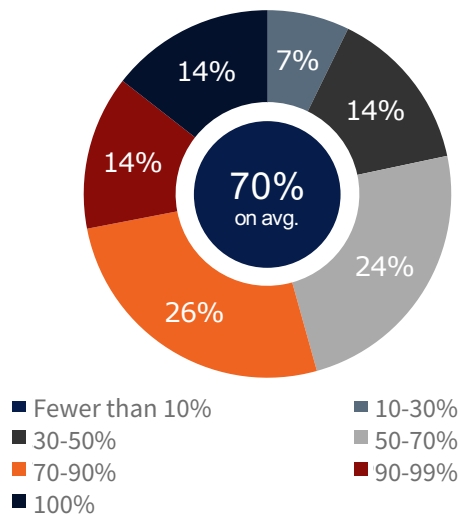
Figure 3: "What percentage of your organization's total email users are using Office 365 Exchange Online?", *asked to respondents from organizations that are currently using Office 365 Exchange Online (346)*

Legend:
- Fewer than 10%
- 10-30%
- 30-50%
- 50-70%
- 70-90%
- 90-99%
- 100%
- Don't know
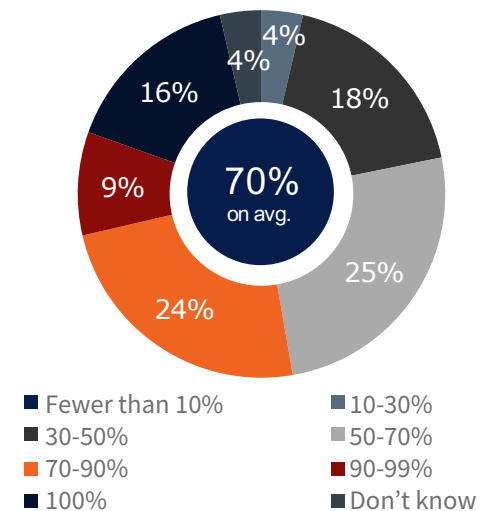
Figure 4: What percentage of your organization's total email users are planned to use Office 365 Exchange Online?", *asked to respondents from organizations that are planning to use Office 365 Exchange Online (220)*
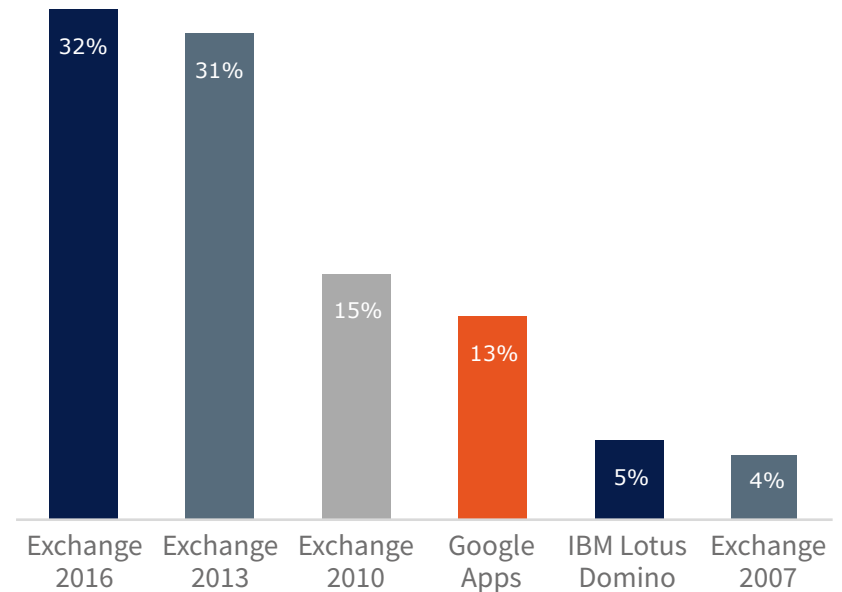
Other email service providers in use

Those who aren't using Office 365 Exchange Online exclusively are using a range of other email service providers.

Around three in ten respondents' organizations currently use Exchange 2016 (32%) and Exchange 2013 (31%). Just over one in ten (13%) are using Google Apps.

This suggests that while not all are solely using Office 365 Exchange Online, most are using an Exchange product of some kind.

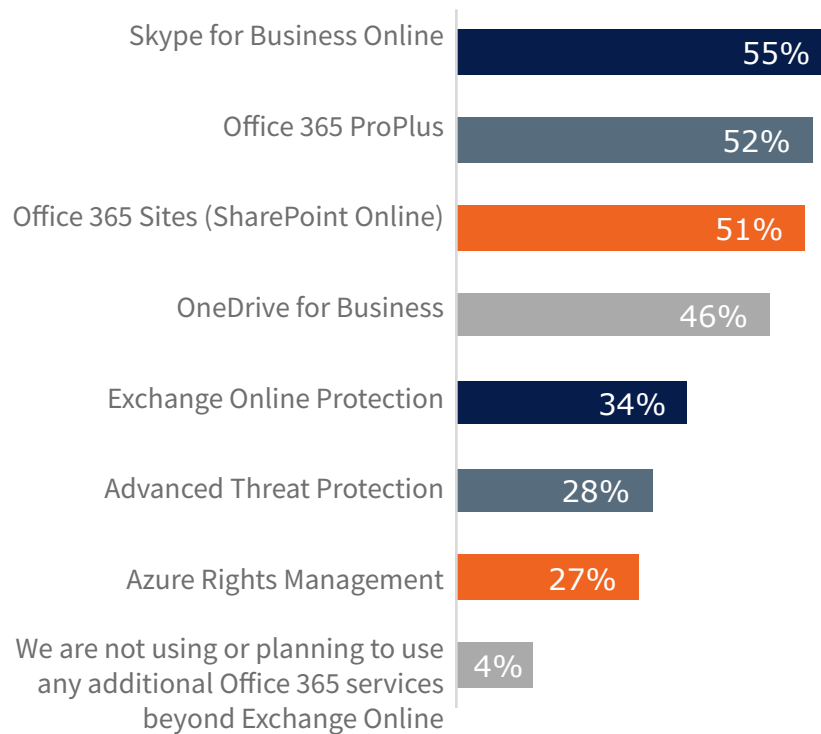Which additional Office 365 services are being used currently or are planned to be used?

Figure 5: "What other email service providers does your organization currently use?", *asked to respondents from organizations that are planning to use Office 365 Exchange Online or if their organization does have it, not all employees are using it (550)*

Additional Office 365 services

Skype for Business Online: **55%**

Office 365 ProPlus: **52%**

Office 365 Sites (SharePoint Online): **51%**

OneDrive for Business: **46%**

Exchange Online Protection: **34%**

Advanced Threat Protection: **28%**

Azure Rights Management: **27%**

We are not using or planning to use any additional Office 365 services beyond Exchange Online: **4%**

Figure 6: "In addition to Exchange Online, which additional Office 365 services is your organization currently using or planning to use?", asked to respondents from organizations that are either currently using Office 365 Exchange Online, or plan to in the future (566)

A range of Office 365 services are being used or are planned to be used by respondents' organizations, in addition to Exchange Online.
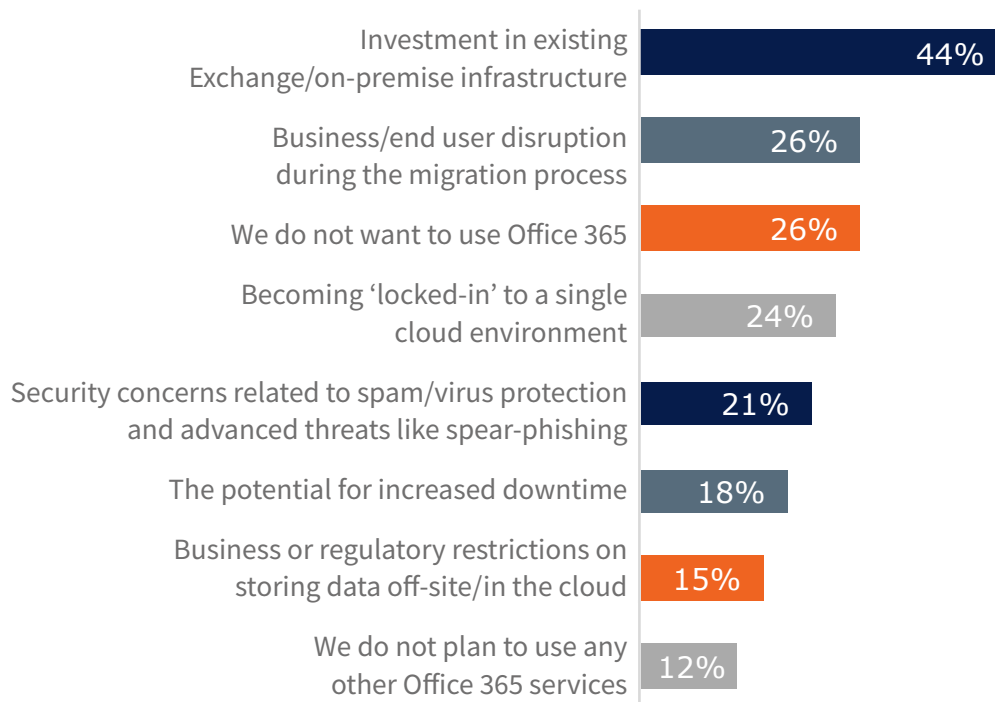
A minority of organizations are using or planning to use Exchange Online Protection and Advanced Threat Protection.

More than half are using Skype for Business (55%), Office 365 ProPlus (52%) and Office 365 Sites (51%).

For those not planning to move to Office 365, what are the reasons?

Reasons for not using Office 365 Exchange

Investment in existing Exchange/on-premise infrastructure — **44%**

Business/end user disruption during the migration process — **26%**

We do not want to use Office 365 — **26%**

Becoming 'locked-in' to a single cloud environment — **24%**

Security concerns related to spam/virus protection and advanced threats like spear-phishing — **21%**

The potential for increased downtime — **18%**

Business or regulatory restrictions on storing data off-site/in the cloud — **15%**

We do not plan to use any other Office 365 services — **12%**

Figure 7: "What are the reasons preventing your organization from moving to Office 365 Exchange Online?", *asked to respondents from organizations that have no plans to use Office 365 Exchange Online (34)*

Only a small proportion (26%) of respondents whose organization has no plans to use Office 365 say that it is simply that they do not want to.

Approaching half (44%) of respondents whose organization has no plans to use Office 365 Exchange Online say that investment in existing Exchange/on-premises infrastructure is preventing them from moving to it. Around a quarter (24%) claim that becoming 'locked in' to a single cloud environment is the reason preventing them doing so.

Most who have no plans to use Office 365 Exchange Online cite having invested elsewhere already as their reason for not moving to it as opposed to having fundamental issues with the product itself.

2: Migration to Office 365

The email migration process

Only around a third (34%) of respondents' organizations used or plan to use a cutover migration, where all users are moved directly to Exchange Online at once.

More than half (51%) used or plan to use a staged migration where some users are moved to Exchange Online and a short-term hybrid environment is maintained while one in ten maintained or plan to maintain a hybrid environment for an extended time period.

This suggests that although some prefer to migrate all users at once, most prefer a hybrid approach of some kind in order to ensure a smoother transition of users and data with minimal disruption.

What will be done with existing email data?
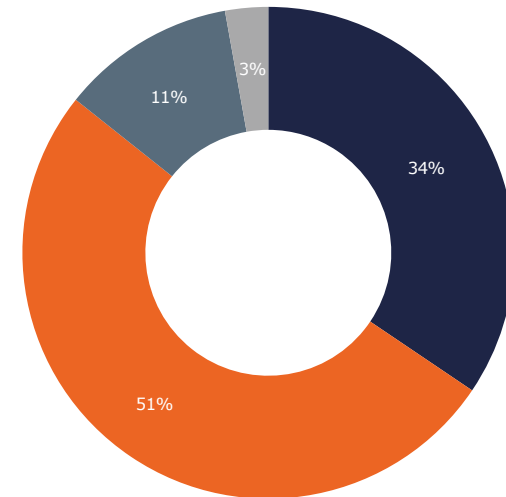
- Use a cutover migration - move all users directly to Exchange Online at once
- Use a staged migration - move some users to Exchange Online and maintain a short-term hybrid environment
- Move some users to Exchange online and maintain a hybrid environment for an extended period of time
- Don't know

Figure 8: "Thinking about the email migration process, which of the below methods did or does your organization plan to use?", *asked to respondents from organizations that are either currently using Office 365 Exchange Online, or plan to in the future (566)*

Existing email data and archived emails
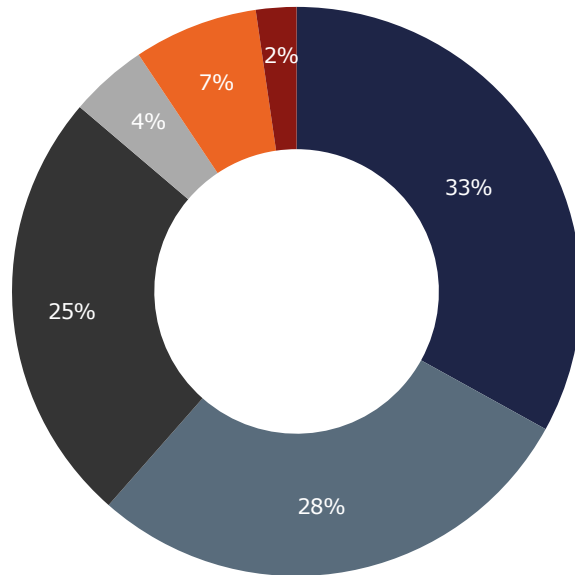
Legend:
- Yes, but only business critical historical email data to Office 365
- Yes, but only business critical historical email data to a third party cloud archive
- Yes, all historical email data to Office 365
- Yes, all historical email data to a third party cloud archive
- No, we will leave historical email data where it is
- Not sure

Figure 9: "In addition to Exchange Online, which additional Office 365 services is your organization currently using or planning to use?", *asked to respondents from organizations that are either currently using Office 365 Exchange Online, or plan to in the future (566)*

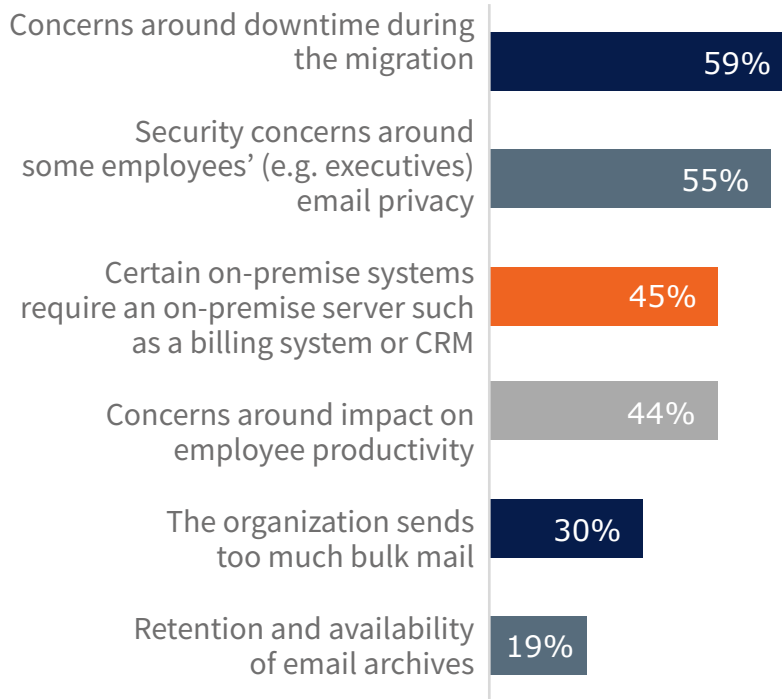## Organizations realize the importance of archived emails.

Most (90%) of organizations that are already using Exchange Online or that plan to in the future have either moved or plan to move some existing email data to the cloud.

However, around six in ten (61%) say that this only applies to business critical email data.

What are the reasons for choosing a staged migration?

Reasons for a staged/hybrid email migration

Concerns around downtime during the migration — **59%**

Security concerns around some employees' (e.g. executives) email privacy — **55%**

Certain on-premise systems require an on-premise server such as a billing system or CRM — **45%**

Concerns around impact on employee productivity — **44%**

The organization sends too much bulk mail — **30%**

Retention and availability of email archives — **19%**

Figure 10: "What are your organization's reasons for choosing a staged/hybrid approach to email migration?", *asked to respondents from organizations that are choosing a staged/hybrid approach to email migration (355)*

The most common reasons for choosing a staged/hybrid approach to email migration are concerns around downtime during migration (59%) and security (55%).

Around four in ten (44%) are concerned about the impact on employee productivity and three in ten (30%) say that a hybrid approach is preferred because their organization sends too much bulk mail.

There are a variety of different reasons for choosing a hybrid migration approach, but most are related to concerns that day-to-day business may be disrupted in some way.

How did organizations undertake their migration or how do they plan to do so?

Methods of executing a migration

A range of different methods are reported by respondents in order to execute email migration.

Office 365 FastTrack (55%) is the most common method used (or planned to be used) by respondents' organizations. But, around four in ten use (or plan to use) third party migration consulting services (41%) and managed service providers (41%).

There is no standout method of executing a migration, but they are taking place with and without the help of external third parties.
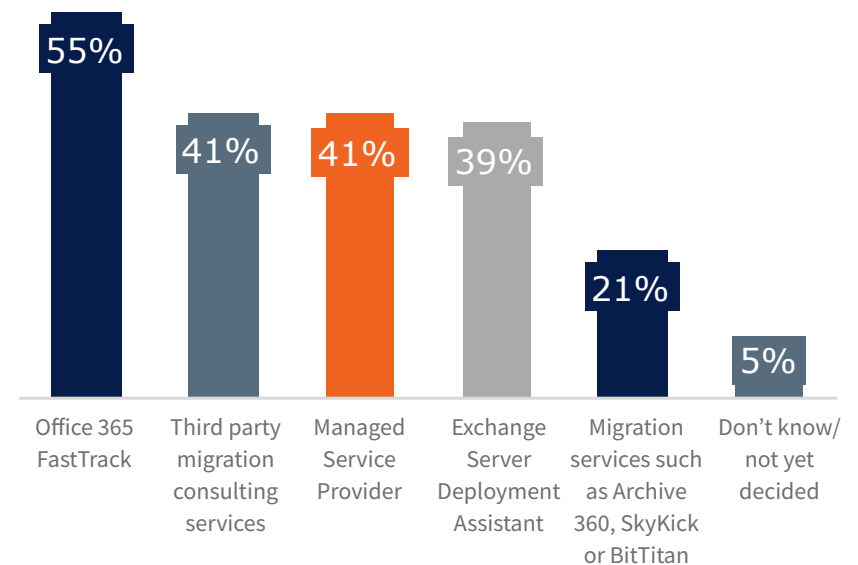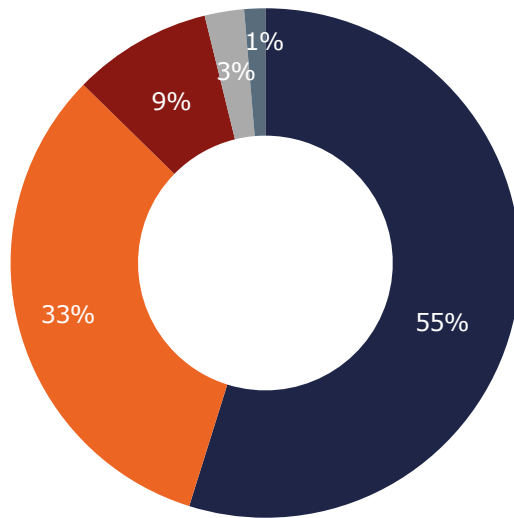

Figure 11: "Which of the following did your organization use (or plan to use) to execute the migration?", *asked to respondents from organizations that are either currently using Office 365 Exchange Online, or plan to in the future (566)*

3: Threat protection

The importance of email availability

- Email is mission critical and we cannot afford downtime
- Email is critical but we accept there will be some downtime from time to time
- Email is important but we are willing to accept periods of downtime
- Email is less critical and our business would not be significantly impacted if it were unavailable for a period of time
- Email is not critical and we would not be impacted if it were unavailable

Figure 12: "How would you rate the importance of email availability to your organization?", *asked to all 600 respondents*

The majority (88%) of respondents rate email availability as being critical to their organization.

Over half (55%) rate email availability as mission critical, saying that downtime is not acceptable.

The importance of email availability may be why respondents' organizations feel more driven towards pursuing a hybrid approach (figure 8), given the concerns felt (figure 10).

What concerns are there in terms of email management capability gaps when it comes to Office 365 Exchange Online?
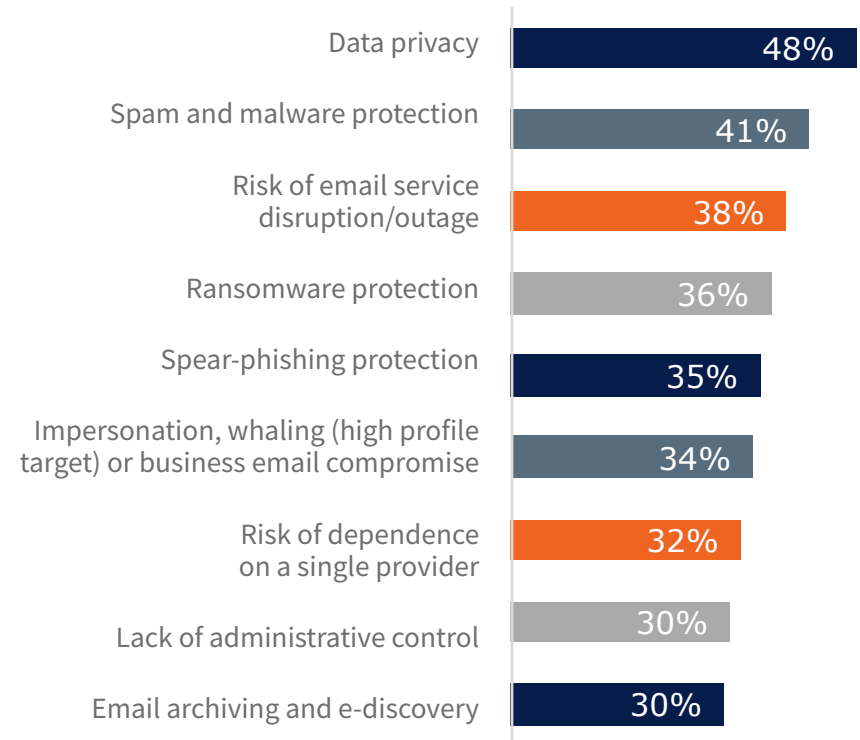
Email management capability gaps

Despite the widely anticipated adoption, many respondents do have concerns when it comes to using Office 365 Exchange Online.

Around half (48%) are highly concerned about potential email management capability gaps relating to data privacy. Around four in ten consider spam and malware protection (41%) and risk of email service disruption/outage (38%) to be high concern.

Given email's high level of criticality to organizations (figure 17), it is perhaps not surprising to see respondents demanding even more from their email service provider of choice and not simply being satisfied with what they are getting.

Are any other non-Microsoft solutions being used to make email safer within organizations?

Data privacy	48%
Spam and malware protection	41%
Risk of email service disruption/outage	38%
Ransomware protection	36%
Spear-phishing protection	35%
Impersonation, whaling (high profile target) or business email compromise	34%
Risk of dependence on a single provider	32%
Lack of administrative control	30%
Email archiving and e-discovery	30%

Figure 13: *Analysis of potential email management capability gaps that respondents consider 'high concern' when it comes to using Office 365 Exchange Online for their organization, asked to all 600 respondents*

Non-Microsoft solutions used to make email

Spam and virus protection — 74%

Advanced threat protection against phishing/spear phishing, ransomware and impersonation attacks — 57%

On-premises archiving solution — 53%

Disaster recovery — 41%

Off-premises (cloud) archiving solution — 35%

We are not using any non-Microsoft solutions to make emailsafer — 4%
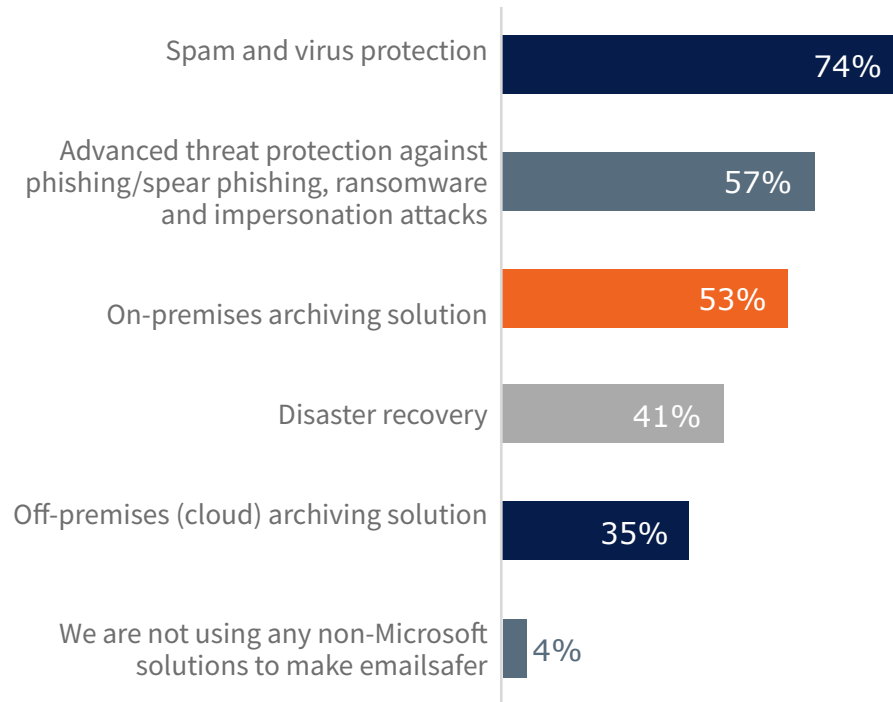
Figure 14: "In your organization's email environment, which non-Microsoft solutions are in use to make email safer for your organization?", *asked to all 600 respondents*

Almost all (96%) respondents' organizations are using non-Microsoft solutions to make email safer.

Around three quarters (74%) are using spam and virus protection solutions.

Over half are also using advanced threat protection software (57%) and on-premises archiving solutions (53%), while around four in ten (41%) are using disaster recovery.

Most are not fully confident in just using the built-in security solutions that their email service provider offers. A variety of non-Microsoft solutions are being used alongside these to enhance email safety.

Are organizations planning to augment built-in Office 365 capabilities through the help of third parties?
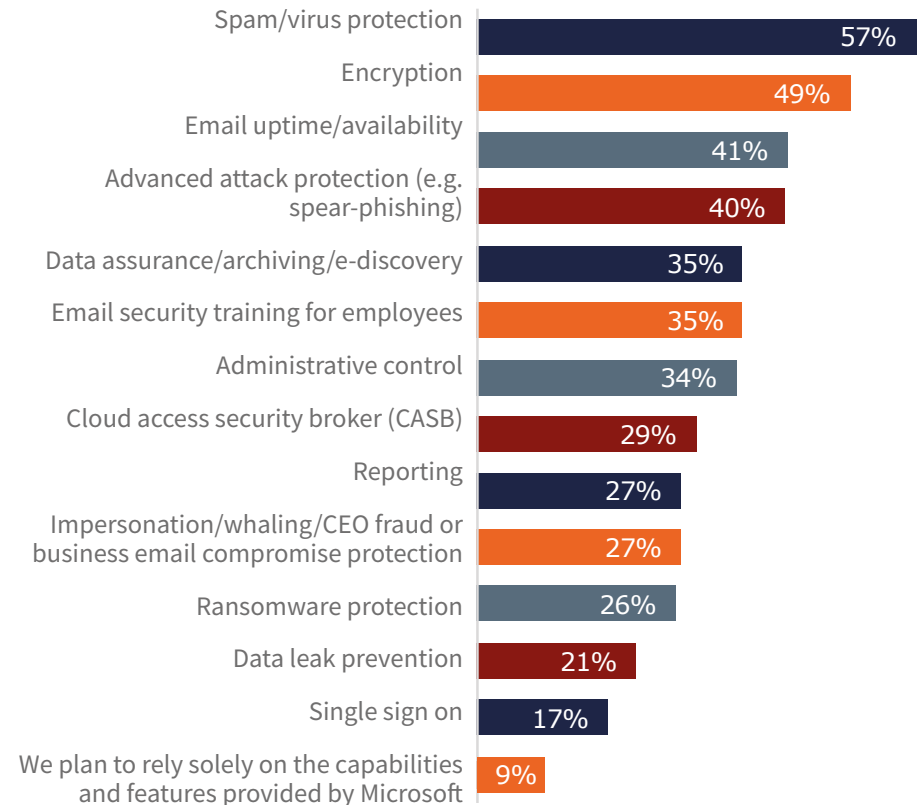
Augmenting built-in Office 365 capabilities

Over nine in ten (91%) will use third parties to augment built-in Office 365 capabilities in some way.

On average, respondents' organizations that are either currently or planning to use Office 365 Exchange Online will augment built-in capabilities to strengthen around three areas:

Strengthening spam/virus protection (57%)
Encryption (49%)
Email uptime/availability (41%)

This suggests that organizations are very open to using third-parties to protect and improve their highly critical email environments.

Spam/virus protection	57%
Encryption	49%
Email uptime/availability	41%
Advanced attack protection (e.g. spear-phishing)	40%
Data assurance/archiving/e-discovery	35%
Email security training for employees	35%
Administrative control	34%
Cloud access security broker (CASB)	29%
Reporting	27%
Impersonation/whaling/CEO fraud or business email compromise protection	27%
Ransomware protection	26%
Data leak prevention	21%
Single sign on	17%
We plan to rely solely on the capabilities and features provided by Microsoft	9%

Figure 15: *"Through the use of third parties, does your organization intend to augment built-in Office 365 capabilities to strengthen any of the below?", asked to respondents from organizations that are either currently using Office 365 Exchange Online, or plan to in the future (566)*

4: Challenges with email providers

Disruption to the Office 365 Exchange Online
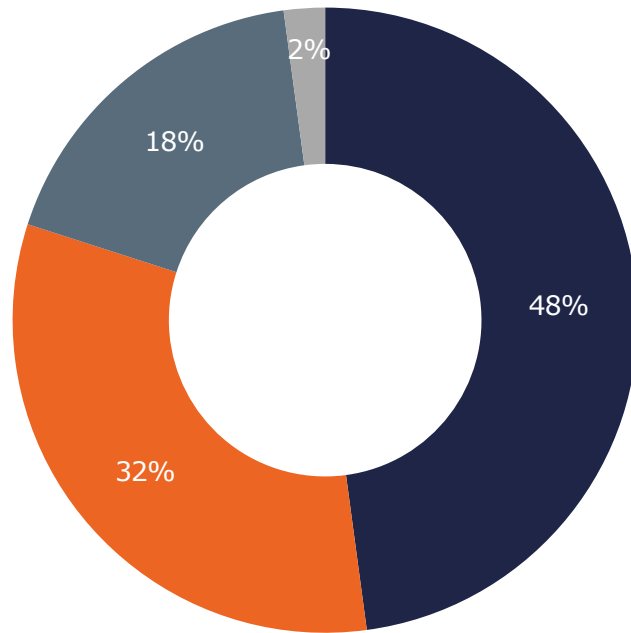
- ■ Wait for Microsoft to restore the service
- ■ Look to a third party to help ensure users can always access their email
- ■ Use a third party monitoring service such as eNow or 365 Monitor to identify potential problems
- ■ We would not take any action

Figure 16: "In the event of a disruption to the Office 365 Exchange Online service making it unavailable to users, which of the below actions would your organization take?", *asked to respondents from organizations that are either currently using Office 365 Exchange Online, or plan to in the future (566)*

If faced with disruption to the Office 365 Exchange Online service, around half (48%) would wait for Microsoft to restore the service.

However, a similar proportion (50%) will enlist third-party assistance to ensure that their users are as unaffected as possible.

This suggests that there is no obvious course of action when disruption to the Office 365 Exchange Online service occurs. Respondents' organizations are split between waiting for Microsoft to fix the problem and taking matters into their own hands by seeking third party assistance.

What technical problems have been experienced when using Office 365 Exchange Online?
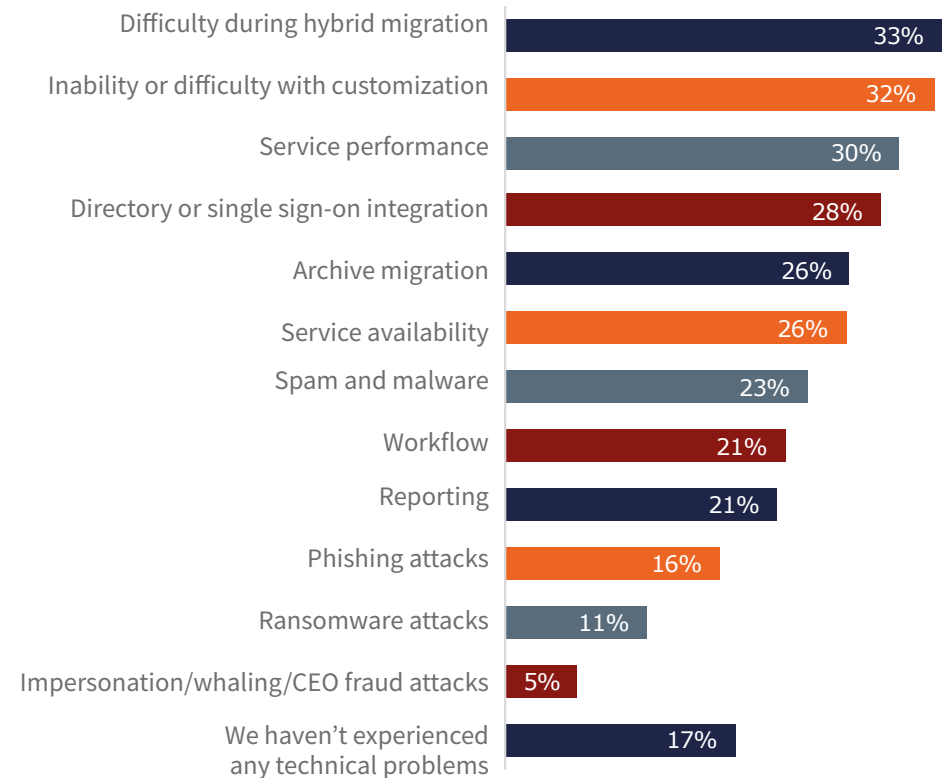
Technical problems when using Office 365

The majority (83%) of Office 365 Exchange Online users have experienced technical problems…

However, there is no single technical problem that stands out above the rest. A wide range have been experienced.

Around one in three have encountered difficulty during hybrid migration (33%), inability or difficulty with customization (32%) and service performance issues (30%).

This suggests that there is not one single defined cause of technical issues with the product, moreover users are faced with different issues related to their organization's own situation and capabilities.
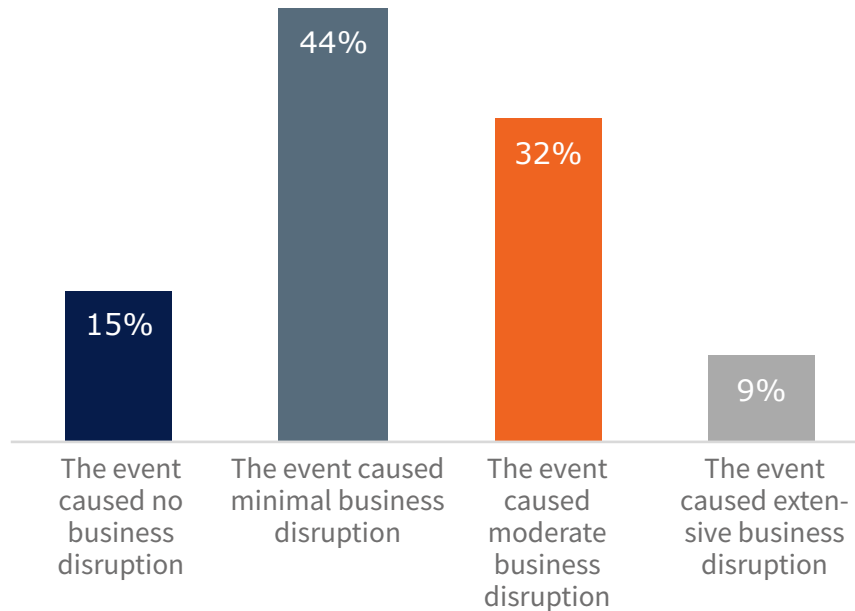
What level of disruption do email outages cause?

Category	Percentage
Difficulty during hybrid migration	33%
Inability or difficulty with customization	32%
Service performance	30%
Directory or single sign-on integration	28%
Archive migration	26%
Service availability	26%
Spam and malware	23%
Workflow	21%
Reporting	21%
Phishing attacks	16%
Ransomware attacks	11%
Impersonation/whaling/CEO fraud attacks	5%
We haven't experienced any technical problems	17%

Figure 17: What, if any, are the main technical problems that your organization has experienced with Office 365?, *asked to respondents from organizations that are currently using Office 365 Exchange Online (346)*

Disruption caused by email outages

44%

32%

15%

9%

The event caused no business disruption

The event caused minimal business disruption

The event caused moderate business disruption

The event caused exten-sive business disruption

Figure 18: "How significant would you rate the event that impacted productivity the most in terms of the level of disruption caused?", asked to respondents from organizations that have been impacted by an Office 365 Exchange Online outage or mail disruption or impacted by another email service provider (197)

Email outages cause significant business disruption.

Over one in ten respondents report that the email outages their organization has suffered caused moderate or extensive disruption.

Only 15% report the event caused no business disruption.

How many outages/mail disruption events are organizations being impacted by?

Number of outages/disruptions experienced

The majority (91%) of those that have been impacted by an email outage have experienced at least one in the last 24 months.

On average, outages/email disruption events were experienced by respondents' organizations three times in the last 24 months.

Not only are these outages causing organizations to experience business disruption when they do happen (figure 27), but they are happening more than once a year.

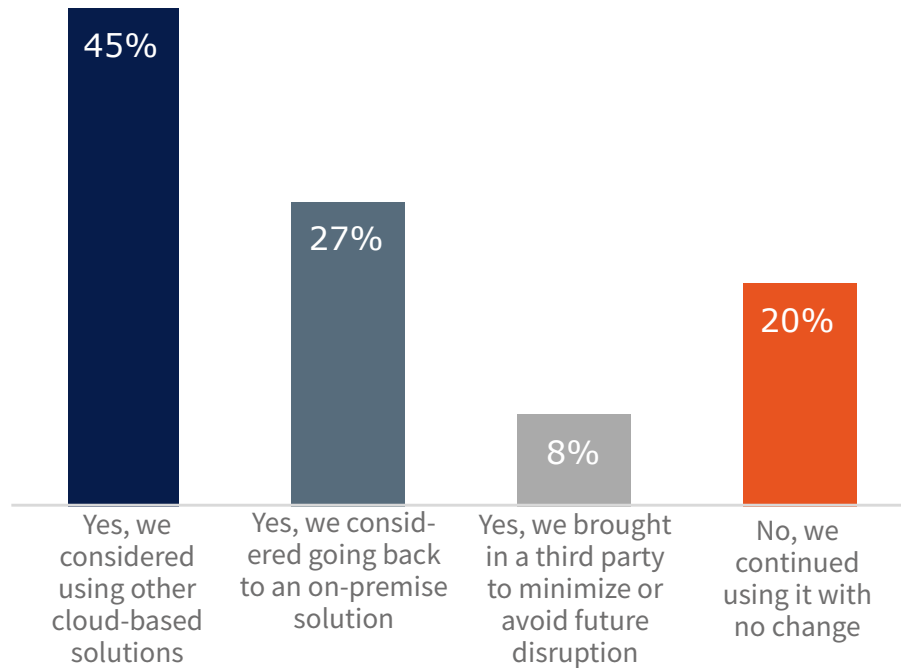Are these disruptions causing organizations to rethink their Office 365 Exchange Online use?
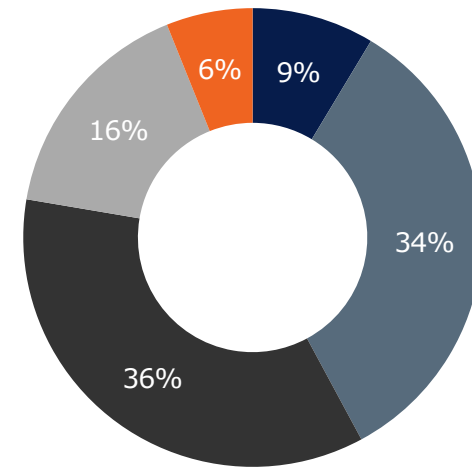
■ None in the last 24 months ■ 1-2 ■ 3-4 ■ 5-6 ■ 7-10

Figure 19: "How many outages/mail disruption events has your organization experienced in he last 24 months?", *asked to respondents from organizations that have been im pacted by an Office 365 Exchange Online outage or mail disruption or impacted by another email service provider (197)*

The outcome of disruptions

45%	27%	8%	20%
Yes, we considered using other cloud-based solutions	Yes, we considered going back to an on-premise solution	Yes, we brought in a third party to minimize or avoid future disruption	No, we continued using it with no change

Figure 20: "Did the disruption cause your organization to rethink its use of Office 365 Exchange Online?", *asked to respondents from organizations that have been impacted by an Office 365 Exchange Online outage or mail disruption (110)*

Four in five (80%) of those affected by outages or mail disruptions rethought their use of Office 365 Exchange Online as a result.

Approaching half (45%) considered using other cloud-based solutions, while around a quarter (27%) considered reverting back to an on-premises solution.

This suggests that while most are either using or planning to use Office 365 Exchange Online (figure 2), problems with disruption and outages may still cause them to reconsider given the high importance of email to their organization's day-to-day operations.

Attitudes to Office 365

Most (73%) believe that their organization still needs to build additional security protections around their Office 365 Exchange Online use.

In the event of an outage, around seven in ten (72%) would feel entirely at Microsoft's mercy to resolve the issue.

Almost six in 10 feel that switching to Office 365 was a management decision rather than an IT decision.

The responses seem to suggest that Office 365 was decided on by management, but that many feel it needs to be protected.

I believe my organization must build additional security protections around Office 365 — **73%**

In the event of an Office 365 email outage, I would feel entirely at the mercy of Microsoft to resolve the issue — **72%**

Switching to Office 365 was/is a management decision rather than an IT decision — **58%**
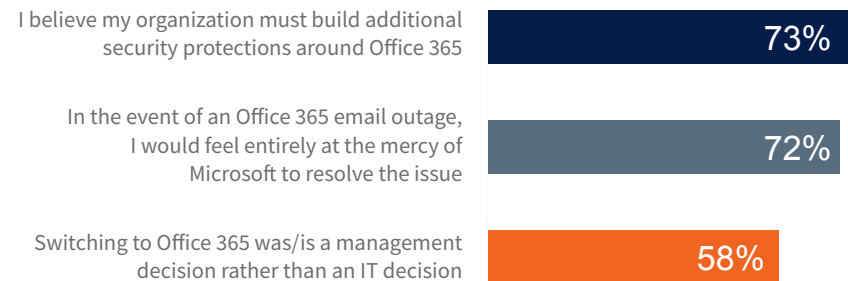
Figure 21: What, if any, are the main technical problems that your organization has experienced with Office 365?, *asked to respondents from organizations that are currently using Office 365 Exchange Online (346)*

In summary

The vast majority (94%) of respondents' organizations either use or plan to use Office 365 Exchange Online.

- Many are also considering using additional Office 365 workloads such as Skype for Business, ProPlus or OneDrive.
- While the most common reason for not using Office 365 is that existing on-premises infrastructure investments are not depreciated, suggesting that more will move in the future.
- Respondents say on average that 70% of the total email users at an organization are on or will be on Exchange Online.

9 in 10 (91%) will use third parties to augment built-in Office 365 capabilities in some way.

- Almost 75% believe additional security protections around Office 365 are necessary.

Most (51%) respondents report that their organization prefers a hybrid, cautious approach to email migration.

- 90% plan to move existing email archives to the cloud.
- The preference for a hybrid approach is driven largely by fears about disruption, security and productivity.

According to respondents, most organizations consider email to be critical, reinforcing the preference for more cautious, hybrid migrations.

- 87% rate email availability as critical to the organization.

If disruption occurs, many respondents say that they are willing to take action and bring in a third-party to assist.

- Mail outages are likely to cause varying degrees of disruption to the business, sometimes leading organizations to reconsider use of their email service provider.

mimecast®

Research conducted by Vanson Bourne:

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com