Chapter 2: Making the Decision to Embrace the Cloud

Tony Redmond

No one likes making an ill-informed decision, especially when that decision is fundamental to a facility that a company depends on. Email often falls into this category. Deciding to move from an on-premises implementation to the cloud, including the possibility of creating a hybrid environment, is a fundamental step. Companies have their own reasons to consider moving to the cloud. Sometimes it is because their IT infrastructure is old and unsupported, as in the case of those running now unsupported servers. Sometimes it is because they face the need to perform a complex upgrade to the latest version of on-premises server technology coupled with the deployment of new server and storage hardware, and the choice to use Office 365 seems easier and more straightforward. And sometimes it is because people consider applications like email and document management to be utility functionality that is better bought from Microsoft instead of being run in-house.

In this chapter, we consider some of the common arguments advanced when people go through the intellectual process of figuring out whether on-premises or cloud technology is best for them. Like any other case advanced about technology, it is critical that you put these arguments in context for your company. Your knowledge about how the company works and its business goals will help you put the points made here into context. Never take a consultant's opinion as definitive!

Removing Cloud FUD

The use of fear, uncertainty, and doubt is a much-beloved tactic to delay or deflect a decision away from certain technology. Salespeople have used FUD since the mainframe era to discourage the adoption of PCs, mini-computers, client-server implementation, the web, social networking, mobile devices, and now the cloud. Some of the fears expressed in the past are still valid concerns and should be considered when any decision to move to a platform like Office 365 is contemplated; other fears are over-hyped.

Common doubts include:

- You can't depend on the cloud (or the Internet).
- Cloud services are immature.
- Cloud platforms are insecure.
- On-premises IT delivers superior service to the company and end users.
- You lose control when you move to the cloud.

It's likely that other concerns will arise. After all, we are talking about technology. In each case, it is important to separate fact from fallacy. Let's look at each of the issues listed above.

Dependability

"You can't depend on the cloud" can have several meanings. It could be that a lack of trust exists that users can connect to cloud services as easily as they can with on-premises services. It could also mean that you think your IT department can deliver a more robust service than you can get from a cloud provider.

There is no doubt that the network is the essential link between cloud services and end users. Three parts come together to deliver end-to-end network connectivity: the internal network used within your company, including the connection to the internet; the internet; and the network controlled by the cloud provider. As explained later, the performance and throughput of any company network that predominantly focuses on in-house systems usually needs upgrading and some tweaking to accommodate Office 365. This is logical – traffic that once flowed to on-premises Exchange and SharePoint servers now goes to their online equivalents. In addition, you can expect more external network traffic from by tasks such as hybrid connectivity, directory synchronization, and remote administration, not to mention the transfer of data from on-premises to cloud platforms (and possibly vice versa). Moving work off old file servers to SharePoint Online and OneDrive for Business also creates traffic, as does the synchronization of documents back to user workstations. New applications like Teams and Planner can create further demand.

Anyone who plans to move to Office 365 needs to pay attention to their internal network and to their Internet connectivity to ensure that enough high-quality network resources are available to handle the expected load. For instance, is enough capacity available to handle the outbound traffic to Office 365 or how many access points exist to process internet traffic? It is often a project management and budget issue rather than a technical challenge.

You can upgrade and revamp an internal network, but you can do little about the internet. It is true that some locations are still badly connected to the Internet (the notion of a stretched string comes to mind), where the connections are barely able to cope with some web browsing and transmission of email back to a central in-house server. If a company has people working in remote offices where only poor network connections are available, then cloud services are probably a bad choice. This situation might well change as the focus on user access shifts away from PC to mobile devices and mobile networks take the place of traditional WAN connections to offices.

However, it is fair to say that Internet connectivity is improving all the time, and this should become less of a factor over time. I have connected to Office 365 using different PCs from multiple locations all around the world and never had much of a problem, even if I had once to resort to running the basic version of OWA through the browser of a Linux-powered smart TV in a hotel in Abu Dhabi. Office 365 applications still worked, albeit slowly. Connecting to Office 365 when you are on the road is not an issue if you can get to a Wi-Fi access point and connect to a public (free or paid) network.

Microsoft accelerates user connections to Office 365 through a network of connection points designed to transfer inbound connections into their network as quickly as possible. This is not an unusual situation as services like CompuServe used similar points of presence (local telephone numbers) several decades ago. Once inside Microsoft's network, traffic flows across connectors with enormous capacity to the Office 365 datacenters. Microsoft experiences occasional glitches in this network but enough capacity and alternate network paths exist to handle most issues.

The second aspect of dependability can be captured as the quality of the service delivered by Office 365. Let's talk about the Service Level Agreements (SLA), the formal agreement that Microsoft makes with Office 365 customers to describe what they will deliver and how they measure the reliability of their service.

Maturity of Cloud Platforms

The second issue often raised by cloud doubters is the assertion that the platform is immature. In other words, the technology used in on-premises deployments is better understood because it has been used for so many years and all its challenges have been met and overcome. It is true that on-premises technology is a well-understood art and that a huge amount of documentation and advice exists to offer best practice for various applications, operating systems, and other aspects. However, it is also true that on-premises deployments suffer from inconsistency. Some are excellent and exhibit all the desired characteristics of attention to detail, superb execution, operational maturity, and dependable delivery of service to end users. On the other hand, there are many on-premises deployments that do not function as well as they might and will take some work to improve before they can consider moving to any other platform, whether that is to use a new on-premises version of Exchange, a hybrid deployment, or moving everything to the cloud.

Cloud services tend to run at massive scale, something that is impossible unless all the characteristics listed above are present. Although automation helps to improve reliability, datacenter operations have not typically posed a problem for cloud services. Software has been more challenging. Specifically, software that was not designed or written to handle the demands of massive scale, multiple tenants, data isolation, security, and global distribution. As the engineers discovered, it is one thing to create an enterprise application like Exchange 2003 that was quite capable of handling the demands of what was then the world's largest Exchange deployment (in the order of 500,000 on-premises mailboxes); it is quite another matter to come up with software that delivers the same functionality to tens of thousands of tenants spanning tens of millions of mailboxes distributed around the world. Hiccups occurred along the way because the software was immature in a cloud sense, but the technical innovation and advances that we have seen in products such as Exchange and SharePoint as well as the evolution of Windows (without PowerShell it's hard to know how Microsoft's commercial cloud platforms could run) over the last ten years have created what we know as Office 365 and Azure today.

Although some might have questioned the wisdom of moving workload to services like Office 365, you can't argue the results. Cloud platforms deliver highly functional software in the form of highly accessible applications across the Internet and do so with a level of reliability and security that would be the envy of many CIOs responsible for internal IT systems.

Security of Cloud Platforms

No organization will move to the cloud if they believe that their data will be less secure than it is on-premises. The same is true for data privacy, as no one wants their information to be exposed to others, including government agencies. Microsoft is fortunate that some of the world's leading security experts work there, including those whose expertise lies in breaking into computer systems. That expertise is used to construct the barriers that protect customer data within Office 365.

Microsoft's official stance is that Office 365 workloads are designed and implemented per the Microsoft Security Development Lifecycle. This is described as "*a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.*" On a practical level, this means that data is secured by being encrypted at rest, that auditing information is available, and that the Office 365 management activity API is supported to allow customers and third parties programmatic access to information protection and compliance events. For instance, BitLocker is used to protect Exchange Online databases (see below) while files stored in SharePoint Online and OneDrive for Business libraries are individually secured with their own 256-bit Advanced Encryption Standard (AES) key.

Apart from some broad guidelines, Microsoft does not usually provide specific details about the methods used to protect information in Office 365 because that could potentially undermine security by revealing too much to those who might contemplate attacking the service. However, a reasonable amount of information, including several white papers that address the security topic in depth, is available in the Office 365 Trust Center. For example, details of the data encryption technologies used by different Office 365 workloads is available online as is a white paper describing how Microsoft uses encryption to protect customer data. The completeness of the security features developed for Exchange Online and Office 365 in general was enough to warrant inclusion of Microsoft in the "leaders" section of Gartner's 2015 Magic Quadrant for Secure Email Gateways, a status Microsoft has held since.

The methods used to protect Office 365 data include:

- **Physical security**: Anyone who has ever visited a Microsoft datacenter can attest to the extremely high level of security processes and procedures that apply. Access is strictly controlled to the servers and other hardware and every action is verified and logged. Any faulty disk drives are removed and demagnetized before they are destroyed to ensure that no possibility exists that customer data might be compromised.
- Very few Microsoft employees have persistent administrative access to applications or the servers running in the datacenters. Although this means that it can sometimes take Microsoft longer than you anticipate to resolve support calls, restricting access ensures that any interaction with customer data is controlled (and audited). The **Lockbox** process ensures that administrators hold zero standing permissions, which removes the problem of how to control the growth of those holding elevated permissions over time. Administrators receive just-in-time permission to perform tasks and have the permissions removed when the task is complete. A similar approach allows customer control over requests for access to tenant data. Any time an Office 365 engineer needs access to tenant data, a request appears in the Office 365 Admin Center for a tenant administrator to review and authorize (or deny). The idea is to give an added level of customer control over their data, hence the name "customer lockbox". The Customer Lockbox feature works for Exchange Online, SharePoint Online, and OneDrive for Business data and is bundled in the E5 plan. You can also buy Lockbox as an add-on for any Office 365 enterprise plan.
- Microsoft audits all access to tenant data and takes great care to ensure that data cannot leak from one tenant to another (see this document for more information about how tenant data is isolated within Office 365).
- Transport Layer Security (TLS) encryption protects information sent between the Office 365 datacenters and clients and messages sent between Exchange Online tenants. You can also create transport connectors that use TLS to protect messages sent to specific domains, such as those belonging to trusted partners. Any client, including browsers, that connect to Office 365 must use TLS 1.2 as Office 365 services will not support connections using earlier versions of TLS from October 31, 2018.
- Data at rest with the Office 365 datacenters is protected by BitLocker. Protection covers both Exchange Online mailbox databases and SharePoint Online and OneDrive for Business document libraries. These steps ensure that rogue administrators cannot remove customer information from Office 365 to sell it on to other parties or otherwise misuse the content.
- Users can choose to protect or encrypt messages using Azure Information Protection, or S/MIME.
- To be complete, you might include features such as Data Loss Prevention (Chapter 22), Advanced Threat Protection (Chapter 17), and classification labels (Chapter 19) in the overall assessment of security capabilities.
- Office 365 depends on Azure Active Directory, which has its own set of protections. For more information, see this whitepaper.
- Microsoft's Privileged Access Management feature (currently in preview) allows E5 tenants to control administrative access to PowerShell cmdlets that create or edit data. Administrators must request access to specific functions and give a reason for the access. After review, the access might be approved, in which case the administrator can go ahead and execute the task. The first version of Privileged Access Management covers Exchange Online, with plans to cover other workloads over time.

Table 2-1 summarizes the different encryption technologies deployed to protect data in different Office 365 workloads.

Encryption technology	***Workload protected***	***Algorithm***	***Key management***	***FIPS 140-2 Level 2 validated***
BitLocker	Exchange Online mailbox databases	AES 256-bit	Windows Certificate Store. The credentials to access the store cannot be obtained without elevated approval within Office 365 management. All access is logged.	Yes
	SharePoint Online databases	AES 256-bit	As for Exchange Online	Yes
	Skype for Business Online	AES 256-bit	As for Exchange Online	Yes
Per-file encryption	SharePoint Online (including OneDrive for Business)	AES 256-bit	Master keys used to protect the per-blob keys are held in two locations: the secure store (native to SharePoint), and the secret store. The keys are updated every 60 days.	Yes
	Skype for Business Online	AES 128-bit	Each piece of content is encrypted using a different randomly generated key. The key is stored in a corresponding metadata XML file that is encrypted by a per-conference master key, which is randomly generated for each conference.	No
TLS between Office 365 and clients	Exchange Online	Opportunistic TLS 1.2 using an AES 256-bit cipher.	The TLS certificate for outlook.office.com is a 4096-bit SHA256 RSA certificate.	Yes
	SharePoint Online		The TLS certificate for *.sharepoint.com is a 4096-bit SHA256 RSA certificate.	Yes
	Skype for Business Online	TLS for SIP communications and PSOM data sharing sessions	The TLS certificate for *.lync.com is a 4096-bit SHA256 RSA certificate.	Yes
TLS between Microsoft datacenters	Exchange Online, SharePoint Online, and Skype for Business Online	TLS 1.2 with AES 256 Secure Real-Time Transport Protocol (SRTP)	Microsoft uses an internally managed and deployed certification authority for server-to-server communications between datacenters.	Yes
Azure Rights Management Service	Exchange Online, SharePoint Online, and OneDrive for Business	Supports Cryptographic Mode 2. RSA 2048 is used for signature and encryption, and SHA-256 for signature hash.	Managed by Microsoft or by customers through a bring-your-own-key (BYOK) process. Thales HSM devices protect the keys. See Chapter 24 for information about some significant reduction in Exchange Online functionality when BYOK is used.	Yes

Table 2-1: Encryption technologies used to protect Office 365 workloads

Although the information presented in Table 2-1 is correct at the time of writing, this is an area that is prone to change as technologies evolve to deal with new threats. Some differences also exist in the implementation used to support government tenants to satisfy specific requirements. The data used by applications built on top of individual workloads are protected by the arrangements put in place for the different workloads. For example, the data used by Office 365 Groups are protected by Exchange Online and SharePoint Online.

The automated workflow engine for Office 365 operations described in Chapter 1 ensures that servers run known configurations. The automated and ongoing updating of servers with new versions of the operating system and applications means that a high degree of confidence exists that known bugs are not met in production.

Industry Standards

None of the practices used by Microsoft are rocket science. Although implemented at massive scale and with huge attention to detail, the practices followed to protect and secure data inside Office 365 are well-known and can be implemented by any company (and indeed, Microsoft documents how they handle security incidents reported for Office 365). The one exception to this statement is found in the background knowledge within Microsoft about the applications and environments running within Office 365. This information gives Microsoft an advantage when it comes to protecting information during operations and is clearly not available within on-premises customers.

Of course, reassurance gained by consulting a web site is not really what you need. Independent auditing is done to ensure that Microsoft adheres to standards such as:

- ISO 27001/27002: Information Management Security System and Best Practice for Security Controls.
- SSAE 16 SOC1 Type II: Reporting on Controls at a Services Organization.
- NIST 800-53: Security and Privacy Controls for (U.S.) Federal Information Systems and Organizations., Microsoft's audit controls for Office 365 are based on the NIST 800-53A (Rev. 4) special publication. The results of the external audit showing how Microsoft's internal control system meets this standard are available in the **Audited Controls** section of the Security and Compliance Center.
- HIPAA: U.S. Health Insurance Portability and Accountability Act.
- The HITRUST Common Security Framework.

A complete set of documents describing how Office 365 meets regulatory requirements and security standards can be found in the Office 365 Service Trust Portal, including the latest audit reports covering Office 365 and other Microsoft cloud properties. Another set of documents helps customers perform a risk assessment and understand the compliance of Microsoft cloud services with industry standards and regulations. Microsoft sets out its approach to securing online services in documents such as the Operational Security for Online Services Overview to help customers understand the policies that it uses to secure Office 365 and other Microsoft commercial cloud services like Dynamics CRM and Azure. Microsoft also publishes information about how Office 365 meets requirements that exist in specific geographies, such as the European Union model clauses, which are "*standardized contractual clauses used in agreements between service providers and their customers to ensure that any personal data leaving the EEA will be transferred in compliance with EU data protection law and meet the requirements of the EU Data Protection Directive 95/46/EC*."

The European Union's General Data Protection Regulation (GDPR), effective from May 25, 2018, affects how companies active in the EU gather and handle data. More information on GDPR and how it relates to Office 365 is available from Microsoft in the service trust portal and in Chapter 19. The Microsoft Compliance Manager gives customers a framework to help them organize the steps to achieve compliance with regulations like GDPR.

In addition, industry-specific reassurances are also sought, such as the white paper authored by a U.S. law firm to outline their opinion why the compliance features built into Exchange Online meet the data retention requirements of rule 17A-4 of the U.S. Securities and Exchange Commission (SEC).

Office 365 does not exist in a vacuum and it is important that the other components that services like Exchange Online depend on also receive external oversight and certification. For example, Azure is certified against the ISO/IEC 27018 code of practice for storage of personally identifiable information in public clouds.

Security for more than Office 365: Although Microsoft assigns talented personnel to the tasks of building security solutions and in protecting customer data within Office 365, there is no doubt that sometimes some extra help is necessary for organizations to achieve full protection. For example, Office 365 offers tenants the chance to deploy data loss prevention technology for many workloads, but this technology does not protect all the data that exists within companies. It might therefore be necessary to deploy some other solutions to ensure that sensitive data is not transmitted outside the organization. When a company moves workloads to Office 365, it is wise to consider whether some more protection is needed for the full spectrum of data that is in use.

Companies who need more security than the basic suite delivered in Office 365 have a wide range of options available to them to harden different components. Microsoft Cloud App Security is available to protect cloud applications at an extra monthly cost per user. Other companies who are active in the provision of additional security capabilities for Office 365 include Mimecast, ForcePoint, Proofpoint, and Skyhigh Networks.

Quality of Cloud Services

Quality can be measured in diverse ways. We have already discussed Office 365 performance against the published Service Level Agreement and shown that Microsoft has an excellent track record in this respect. Software flaws is another measurement. In other words, does Office 365 deliver high-quality software that works all the time? No software is flawless, and Office 365 is no different. Bugs exist and become known all the time. Often people don't understand why this is the case and wonder why Microsoft can't stabilize Office 365 so that all bugs are eradicated, and functionality works as documented all the time. Although it would be nice to run services in a bug-free environment, it's not going to happen if four factors exist. These are:

- **Competitive pressures**: Microsoft does not run Office 365 in a vacuum and must respond to technical and feature advances made by its competitors to ensure that Office 365 stays an attractive offering in the market. Once you touch code to improve functionality or "make things better", the possibility exists that bugs creep in.
- **Customers demand more functionality**: Customers also ask for new features in many different areas of Office 365. Requests vary from a slight change to the way some feature works to an update designed to facilitate the onboarding of large enterprise customers. Microsoft monitors support tickets closely to focus in on areas that cause users to have problems (such as deleted item recovery) and makes changes to improve matters.
- **Different clients are in use**: A staggering number of client platform combinations (browser, Windows, mobile) and protocols interact with Office 365. Clients have been known to introduce problems (for example, several Apple iOS upgrades have caused issues for Exchange), and the support and testing matrix is very complex. Testing complexity creates more possibility for bugs to creep into software and stay undetected until a user meets a problem.
- **Software interaction**: Although email is often the first workload moved to Office 365, it is important to view the service as not being a single workload. A better and more productive view takes in Exchange Online, SharePoint Online, Skype for Business Online, Yammer, Azure Active Directory, Azure Information Protection, the Microsoft Graph, Delve, and so on. Behind the scenes, a complex set of interconnections link Exchange Online and SharePoint Online (for features like Office 365 Groups), Exchange Online and Teams (so that conversations are captured for compliance), Exchange and Delve (so that attachments show up in Delve views), and so on. SharePoint Online is the storage for functionality such as the Office 365 Video Portal while Azure storage supports other applications like Planner and Teams. Each of the software applications has their own set of developers, testers, and plans. Maintaining the connections between the different applications can take substantial effort, which is one of the reasons why some of these features are not available on-premises.

We will never be rid of bugs when software evolves and flexes all the time. We accept this situation because we like new features and functionality. Remember that one of the reasons why customers adopt cloud services is the promise of "evergreen technology", to move away from the more restrictive upgrade cycles used in on-premises deployments. With evergreen or ever-evolving technology comes the risk that things don't work quite as well as they should from time to time. That's when you enter the world of cloud support.

Office 365 Support

Microsoft gives free support for Office 365 tenants. Support varies from forum-only to telephone support to online requests for support that flow to dedicated support personnel. Support is often referred to as the "Achilles Heel" of cloud services because it is so difficult to deliver support in a timely and effective manner to tens of millions of consumers. By comparison, on-premises services are often supported by in-house help desks and support teams. A company has control over the quality of those services based on the investment made to staff up the help desk and train support personnel. The transition from a position where you have total control over all the moving parts needed to resolve a support ticket to depending on the intervention of cloud support, when you really do not control a lot, is difficult for many organizations. IT professionals are frustrated with having to deal with phone support, users do not like how long it takes for even simple issues to be resolved, and managers worry about the control they have ceded to the cloud provider.

All of this is true. When you move from a customized in-house solution to use a shared utility infrastructure you must make some adjustment. Think of it like this – if you use a diesel-powered generator to power your house, you have total control over the infrastructure and offer all the support. But when you sign up with a power company, you hand over responsibility for most of the operations to that provider. All you must do is make sure that equipment is plugged in and turned on. The same is true of using a utility IT service. You don't have to maintain the servers or make sure that their networking equipment is functioning, but you do have to ensure that your own equipment is functional.

The horizon for in-house support provided by an IT department changes when workload transitions to the cloud. Instead of driving problems to resolution, you now manage the interaction with Microsoft to work the problem as effectively as you can within the constraints placed on both you and the Microsoft support organization.

You control local equipment and settings and can make sure that you cover all the basics – that the user's client is configured correctly, that they can connect to the Internet, whether the problem is unique to a certain user or is shared by a group. Microsoft support is delivered remotely and will usually be invisible to the end user unless they learn about it when they are asked to check some local setting or variable on their PC. Microsoft owns the responsibility for recording the support ticket and following through until the issue is finally resolved. But you should remember that Microsoft support professionals cannot make changes within an Office 365 datacenter. All they can do is record, probe, and diagnose problems. Sometimes that will be enough to get a resolution and sometimes they will need to escalate from first-level through second-level right up to the elevated heights of the few who can work directly with servers, if that's what is required to fix a problem.

Working a problem through many interactions with different levels of support takes time. Multiple phone calls and email interchanges are likely going to be necessary to keep an issue moving toward resolution. Don't blame the support personnel – they follow a strict playbook to gather information, suggest fixes, and escalate when required. Think of how you'd function if you had to understand the myriad different circumstances that customers who report problems are in. It sometimes takes a lot of time to simply understand what's going on before you can move toward resolution.

Microsoft uses a mixture of subcontractors and Microsoft badged employees to provide first level support for Office 365 (access is described here). First level support is designed to provide first response to incoming calls. The calls are registered in Microsoft's ticketing system and a structured approach is taken to recording details of the incident that can possibly lead to a fast resolution if the problem and its solution is already known. Calls that cannot be resolved by first level staff are escalated to second level support. These individuals have deeper product knowledge and are better able to diagnose and resolve complex support situations. Because Microsoft operates a DevOps model for Office 365, the most difficult calls eventually escalate to the product group responsible for the area where the fault lies. At all times, customer confidentiality and data privacy are respected.

When you report a problem with Office 365 to Microsoft, it is critical that you keep careful notes of the date and time for each call or other contact and record to whom you spoke, what was discussed, what actions should occur, their expected outcome and when this should happen. Apart from simply being good sense to record information about support incidents, this information will be invaluable if you need to request an escalation or wish to review why a problem is not being resolved, perhaps by contacting the supervisor of the support professional with whom you are working.

Communication with end users is critical. They probably won't realize the details of the complexity of cloud services, nor should they be expected to understand the links between the client software that someone wants to use to connect to Office 365. Making sense of the complexity and managing support calls is the new role for the local IT department.

Limited responsibilities: Microsoft makes it quite clear what they will and will not support when it comes to Office 365 calls. The normal guidance is:
"*Escalation scenarios that the Office 365 support team will not accept include but are not limited to the following:*

- *Your networking infrastructure.*
- *Your hardware.*
- *Microsoft on-premises software that is not part of the Office 365 service offering.*
- *Non-Microsoft software.*
- *Your operational procedures.*
- *Your architecture.*
- *Your IT service management process errors, system configuration errors, or human error.*"

The Question of Losing Control

Consumers of cloud services do not get to vote about when functionality is introduced or changed. It just happens, and it is done by the cloud provider to meet their goals and priorities rather than yours. This is part of the contract that you sign and the control that you cede when you decide to start using cloud services instead of your own on-premises service. It is just like what happened when people stopped using their own electricity generators or water pumps and connected instead into the public electric and water utilities. They lost the control over how their generator or pump worked when they traded it for the promise that the service delivered by the utilities would be better, more predictable, and cheaper. Although they could no longer decide on questions such as what fuel is used by the generator or how long a pump ran daily, they still had access to power and water.

Email is very much a utility at this point. SharePoint is less of a utility, but only in parts. Document libraries are a utility, bespoke applications built on top of SharePoint are not. Skype for Business Online is a utility and so is Yammer or Delve. Moving to use cloud-based versions of these applications is very much like making the decision to use a public utility. And yes, a decision to move to Office 365 means that some control is ceded, but most people can cheerfully give up the responsibility for installing the latest versions of Windows and Exchange on a server, bringing it up to the latest patch level, and making sure that any required additional products are installed.

What can be more problematic is when the characteristics of the service change in a way that you prefer it did not. For instance, in February 2015, Microsoft announced that the contents of the Deleted Items folder would no longer be cleared out periodically by the Managed Folder Assistant. This was a great decision for small tenants who often care very little about compliance, but it affected the compliance strategy of many large tenants, especially those who run hybrid environments because different methods of processing the same retention policy then existed on the two platforms. Microsoft made the decision to stop removing items from the Deleted Items folder for their own good reasons, but in effect, this is an example when the interests of small tenants trumped a business and regulatory need of enterprise tenants. However, Microsoft made sure that the change was easy to reverse – if you realized that it had been made.

Another example is illustrated by the situation that occurred for Delve in June 2015. Microsoft found an error in the code that loaded user profiles and acted to fix the problem. The side effect was that the Delve user interface reverted to an earlier version, a change that caused disruption for end users and administrators alike. The problem lasted for five days before the user interface was restored. No warning was given to tenants that the problem had happened and what its effect would be.

The positive way of looking at how things flex and change without warning or any ability to influence an outcome when you use cloud services is to not focus on any loss of control over the servers and other infrastructure that you no longer manage. Instead, focus on how best to use all the added hours that you gain and figure out how to use that time in a more productive manner.

Understanding Service Level Agreements for Cloud Services

Two formal documents govern the provision of Microsoft Online Services to customers. Both documents are updated quarterly. The Volume Licensing Online Services Terms lay out the terms under which Microsoft delivers the service within Office 365. The document is available in multiple languages. More information is found in the Service Level Agreement for Microsoft Online Services, also available in multiple languages. This document explains how Microsoft measures the SLA for its Online Services.

Each of the individual workloads running inside Office 365 has its own SLA definition. For Exchange Online, Microsoft defines downtime to be "*Any period of time when end users are unable to send or receive email with Outlook on the web.*" The actual calculation is a little more complex:

"The "Monthly Uptime Percentage" for a Service is calculated by the following formula:

((User Minutes – Downtime)/User Minutes) * 100

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident."

Not all users are affected by each incident, so the number of user minutes generated by an incident varies. Many of the incidents noted by monitoring products are transient and last just a few seconds and can be put down to a temporary condition that occurred somewhere along the path between client device and server running in an Office 365 datacenter. Over the course of a working day, micro-outages can happen five or six times without causing disruption to end users. Outlook's cached Exchange mode, for instance, enables users to continue working when the server is temporarily unavailable and most mobile devices will reattempt to connect after a short period. These micro-outages can sometimes be detected as a failure of a page to load or a server to respond in a timely manner. They usually resolve themselves without the need to intervene on the part of either Microsoft or the tenant administrator.

Given the massive number of users who access the Office 365 services, it is fair to say that an incident that lasts several hours but only affects a small group of users (for example, in one Office 365 datacenter or region) will not have much effect on the SLA while a global outage can dramatically influence the SLA because so the incident consumes so many user minutes. Due to the distributed nature of the infrastructure, incidents usually stay constrained within a single Office 365 datacenter or even a single Office 365 region. Even the 7-hour

Exchange Online outage from July 2014 that affected North American tenants went by without the rest of the world noticing. The last truly global outages occurred in September 2011. High-profile but region-constrained outages like those that affected U.S. tenants in June 2014 and July 2015 seldom move the SLA needle very much. Indeed, a daily glance at the Office 365 service dashboard will invariably show that at least one of the applications is currently experiencing some level of difficulty that might or might not affect your users. This is part of the joy and the pain of sharing in a massive multi-tenant infrastructure.

If the reported Monthly Uptime Percentage falls under 99.9%, Microsoft guarantees that they will refund customers with a service credit for a set amount ranging from 25% to 100% (for less than 95% availability).

An SLA of 99.9% ("three nines" in high availability parlance) allows a service provider to have downtime of up to 43.8 minutes per month, or 8.76 hours annually. As explained above, lost minutes for Exchange Online accrue when users can't send or receive mail with OWA. For SharePoint Online, it is "*any period of time when users are unable to read or write any portion of a SharePoint site collection for which they have appropriate permissions,*" while for Skype for Business Online it is "*any period of time when end users are unable to see presence status, conduct instant messaging conversations, or initiate online meetings*." These conditions are documented in the Service Level Agreement for Microsoft Online Services.

Counting minutes for SLA calculation only happens when Microsoft support records an incident and accepts responsibility for the problem. In most cases, this means that the problem has to happen within a Microsoft datacenter to a component that is under Microsoft's control. Anything that happens within the control of the customer, such as a misconfiguration of client software or a local network malfunction, does not count against the SLA. This is logical because Microsoft can only be blamed for the parts of the service that it controls.

Microsoft is not the only cloud provider to limit SLA measurement at the boundary of its datacenters. No one controls the Internet, and no one controls how data flows from your client to a datacenter. Many complex steps occur between a client connecting to a cloud service like Office 365, perhaps using multi-factor authentication from a mobile device, to being able to access and interact with data. It is therefore impossible for a provider to offer an SLA guarantee as measured at the client. Well, perhaps possible because anyone can offer such an SLA, but certainly foolish in terms of their chances of ever meeting the SLA.

Microsoft excludes scheduled downtime from any SLA calculation. This is downtime that Microsoft needs to maintain its service and is advised to customers at least five days before it happens. On the other hand, any sudden outage that comes without warning always counts against the SLA, if Microsoft accepts that the incident is caused by their software or infrastructure and did not happen because of an action taken by the tenant.

At any single time, there are multiple incidents unfolding within Office 365. Some of these are very local and affect a single server. Some are more widespread and degrade the service delivered to large numbers of tenants or even stop an application working for those tenants. Some incidents are transient and go away on their own accord and some linger for days, albeit perhaps without affecting tenants. The point is that an infrastructure that is so large cannot run in a perfect state all the time. Because Office 365 depends on hardware, software, and humans, you can be sure that something is always happening for the wrong reason. Of course, users will not care unless an incident stops them sending email, accessing documents, conducting a teleconference, or some other operation.

In most cases, any issue that affects the SLA is soon obvious because users are unable to connect or to do work. Microsoft has automated systems in place to interpret problems and map them against tenants so that the incidents shown up in the Office 365 Admin Center are those that might affect smooth operations for your tenant. Details of incidents appear in the Service Heath Dashboard (SHD). We discuss how the understand the SHD, navigate within it, and file service incidents for your tenant in Chapter 4.

A summary of incidents for the last 30 days is also available in the Office 365 admin portal together with post-incident reports (PIRs) by going to **Service Health** and then selecting View history. However, it is easy to forget to check the portal from time to time to see what the status across all parts of the service. Unless you run a third-party product designed to automate the health state of applications such as Exchange Online and SharePoint Online, it is possible that the first sign you receive of a developing problem is through social media. Some of the third-party monitoring products gather statistics about the availability of Office 365 as viewed through the lens of an individual tenant. That data can be useful when it comes to discussing SLA performance with Microsoft if the need arises to make a claim for poor service.

What is a PIR? A PIR is a Post-Incident Report with the formal analysis of an "*unplanned customer-impacting service incident*" or outage where there was "*broad and noticeable impact across a large number of organizations*." Few incidents that you see in the Service Health Dashboard affect enough tenants for Microsoft to write and publish a PIR. When these incidents do happen, Microsoft makes PIRs available to customers through the service dashboard. The Office 365 support team publishes a preliminary PIR within 48 hours of the incident closure followed up by a full and detailed PIR within five business days. A PIR the following sections:

- **Incident ID**: Every Office 365 incident has a unique identifier. For example, EX29054 is an Exchange Online incident.
- **User Experience**: A brief description of what impact was suffered by end users. It might be that only administrators were affected if the component involved is something like PowerShell.
- **Customer Impact**: What business impact if any was caused by the incident.
- **Incident Start Date and Time**: In UTC format.
- **Incident End Date and Time**: Logically, the difference between the start and end date is the incident period used to calculate time lost against SLA.
- **Root Cause**: Microsoft's explanation why the incident occurred.
- **Actions Taken**: A timeline of all the actions taken from the time when the incident occurred to its resolution. Sometimes several hours go by before engineers have correlated enough data from multiple tenants to be able to home in on the components that might lie at the root of the problem.
- **Next Steps**: What Microsoft proposes to do to ensure that the same problem will not recur.

As in all administrative documents, sometimes you must read between the lines to understand just what happened and why it happened. The PIR also exists in internal and "customer ready" forms, the former being much more detailed than the latter.

Social media is important to Microsoft when it comes to monitoring the service too. The sheer number of users who connect to Office 365 means that any error in the service can quickly escalate to affect millions of people. Microsoft monitors information flowing through social media to detect problems that users report with Office 365. This is just one of the ways that they try to figure out the quality of service delivered to end users. Microsoft does its best to keep the service dashboard updated with information about problems as they arise but because most incidents are confined to a single datacenter or region, it can often be a challenge to understand whether any specific issue affects a specific tenant.

Seeing a tsunami of updates about a problem with Office 365 is not a reason to panic because the problem might not affect you. Remember that Office 365 is deployed in datacenters around the world and that any problem is likely to be localized within one region. In the case of the high-profile incident in July 2014, the root cause was a failure in the Azure Active Directory infrastructure that supports Office 365, but only in the part of the infrastructure dedicated to handling inbound connections from North American users. When the problem happened, the directory service could not handle the volume of validation requests created to check the addresses on inbound email, reducing the ability of Exchange Online to process traffic. It was possible to send and receive some email during the outage, but in most cases, customers had to wait until Microsoft restored the directory service to full health before their email flowed normally.

The average administrator has no real chance of understanding the data used in SLA calculations because much of it is invisible to anyone outside Microsoft. Factors such as Internet outages, local network delays, or client misconfiguration are also excluded from the SLA equation. This means that one tenant might believe that Office 365 delivers an excellent performance against SLA, while another tenant experienced some problems, perhaps some of their own making, and has quite a different perception of the service quality received. Beauty is in the eye of the beholder and it is obvious that the sheer size of Office 365 creates a blurring effect across its regions. Service is excellent overall (as seen in the reported SLA figures) but is awful when experienced by individual tenants affected by different bugs or operational issues.

To be fair to Microsoft, they have met their financial commitment to refund customers when the root cause for obvious Office 365 outages were mistakes that were under their control. It is important to recognize that most outages are of short duration and only affect a small percentage of the overall Office 365 user base.

Office 365 Performance Against SLA

Microsoft reports the SLA performance for Office 365 against its 99.9% target on a quarterly basis. Microsoft aggregates the data for all Office 365 regions to create a worldwide result and does not give SLA information for individual Office 365 regions. Table 2-2 details Office 365 performance against SLA since figures first became available in 2013. The highlighted figure is the most recent published quarterly result from Microsoft.

Q1 2013	***Q2 2013***	***Q3 2013***	***Q4 2013***	***Q1 2014***	***Q2 2014***	***Q3 2014***	***Q4 2014***
99.94%	99.97%	99.96%	99.98%	99.99%	99.95%	99.98%	99.99%
Q1 2015	***Q2 2015***	***Q3 2015***	***Q4 2015***	***Q1 2016***	***Q2 2016***	***Q3 2016***	***Q4 2016***
99.99%	99.95%	99.98%	99.98%	99.98%	99.98%	99.99%	99.99%
Q1 2017	***Q2 2017***	***Q3 2017***	***Q4 2017***	***Q1 2018***			
99.99%	99.97%	99.985%	99.988%	99.993%			

Table 2-2: Office 365 SLA performance since 2013 (source: Microsoft)

The blips in the Q2 2014 and Q2 2015 results are due to some high-profile incidents that deprived some North American customers of access to email during those quarters, allied to a mass of smaller incidents that occurred distributed across the other Office 365 regions. Although many smaller incidents have been recorded since, no major outage has affected SLA results for Office 365 in quite the same manner.

SLA results are available approximately a month after the end of the quarter. Remember that the SLA data reported by Microsoft is a combined view taken from across the complete service. Your tenant might have experienced an inferior level of service in a quarter, but even if a problem affects hundreds of thousands of users for several hours, the sheer scale of Office 365 means that this incident might not be enough to move the needle for the reported SLA.

Making the Decision

So far, we have concentrated on removing some of the FUD that surrounds cloud services. Now let's move on to consider some scenarios when the decisions to embrace the cloud and move to Office 365 is easy as well as when complications might make things a little more "interesting".

The Easy Decision

As you might expect, the decision to move to the cloud is much easier for some companies than it is for others. Broadly speaking and accepting that these are high-level generalizations, the characteristics of companies in this category include:

Start-up companies: Why would any start-up want to create its own IT infrastructure when most, if not all, of the services they might need to use are available in the cloud? Apart from anything else, buying on a fixed cost per month is usually better for cash flow. The exception to the rule is companies who have been created to develop a product associated with an on-premises server product like Exchange. In this case, it is a good idea to eat your own dogfood and run some Exchange servers.

Small to medium companies: Anecdotal evidence shows that much of the initial migration to Office 365 came from companies with less than 500 employees, many of whom had run older generations of Microsoft servers such as Windows Small Business Edition. Replacing old servers (some that resided in the proverbial cupboard or under someone's desk) with the promise of evergreen functionality offered by the cloud is very attractive, especially when the migration of mailbox data is relatively straightforward as the volume is small enough to accomplish a smooth weekend switchover. These companies tend to be "all in" the cloud and don't need to operate hybrid environments so they aren't interested in aspects such as federation and single sign-on. Microsoft provides a FastTrack deployment service to help companies like this who purchase 50 or more Office 365 licenses. The fact that Microsoft considers that many of the onboarding operations necessary to move these companies to Office 365 can be executed on an almost factory-like production-line basis indicates the relative ease the switchover can be, especially for small to medium companies whose needs do not extend past email. More complex email scenarios (for instance, those involving specific regulatory oversight) and SharePoint migration usually need the services of a specialized migration partner.

Fortune 500 companies: Including Fortune 500 companies after small to medium companies might seem strange, but the fact is that most if not all the Fortune 500 companies have some element of work running inside Office 365. Sometimes a tenant domain is taken to reserve it for future deployment. Sometimes it is used to test the waters for a planned move to Office 365. And sometimes it is because the company is in the process of moving some, but probably not all, of its email workload to Office 365. Hybrid deployments are the usual rule of thumb for very large companies in this category because this approach is most flexible and allows transparent co-existence across the two platforms, including a shared directory, integrated mail flow, and access to data.

Moving from a non-Exchange email system: Microsoft supports the migration of IMAP4-based email systems to Exchange Online. Older POP3 accounts are more of a challenge because these must go through an interim step where messages are downloaded to a PST with Outlook and then imported into Exchange Online, again using Outlook. It's a manual process that can be tiresome. Then again, you can simply leave the old mail in the PST and not bother with the import. Migration from other email systems such as Lotus Notes or Novell GroupWise can be done using separate tools bought from companies that specialize in the migration area. Table 2-3 lists some of the well-known companies in this space. Take the time to download trial versions of their software to establish the tool that is the right choice for you.

Company	***Migration Tool***
Binary Tree	E2E Complete
BitTitan	MigrationWiz
Code Two	Office 365 Migration
SkyKick	Enterprise Migration Suite
Quadrotech	Mailbox Shuttle

Table 2-3: Email Migration Software for Office 365

Educational institutions: Many universities and colleges used earlier versions of Microsoft cloud-based email (such as Live @EDU) or have experience running a competitor's cloud-based email. It is obvious that these institutions will find it easy to move to Office 365.

Again, these are generalized comments and individual country-level markets differ in terms of the mix of accounts that have moved to Office 365.

The Harder Decision

The categories listed above are examples of organizations that are relatively easy to move to Office 365. Now let's look at some of the circumstances that can complicate matters.

Multi-location or multi-national: It is obviously much easier to coordinate the movement to Office 365 if everyone (users and IT staff) share a common location. Planning becomes more complex as the number of locations grow and more complex still if multi-national locations are involved. The needs and legal requirements of each country, including security and privacy, should be factored into a migration project.

Email integrated with business processes: Although the API history of Exchange is speckled with false starts and dead ends, there's no doubt that many companies have integrated email with business processes. For instance, when HR registers a new employee, a mailbox is automatically created, and a welcome message is sent to the mailbox. Exchange Online supports EWS and PowerShell and it might be possible to move the email-enabled processes to the cloud. Microsoft's longer-term direction for extensibility is based on the Microsoft Graph covering all the Office 365 workloads. Alternatively, you could keep an on-premises server to handle email for those applications.

More than 25,000 seats: The more mailboxes you must move, the longer a migration to Office 365 will take. Migrations are never popular exercises as they involve lots of repetitive operations (moving mailboxes) that are prone to problems (corrupt items and other issues) that take a long time to achieve, especially when moving mailbox data across the Internet. Given the right experience, good project management, and network connectivity, it is possible to move several thousand mailboxes per week – but it is not easy.

Capable of running an internal cloud: Small companies have small IT departments and the people working in IT are jacks-of-all-trades who are expected to be able to work with many different technologies. Larger companies can afford to have specialists and specialization tends to enable a more sophisticated IT environment. These companies might have the necessary expertise and operational maturity to be able to run an internal cloud where on-premises versions of products like Exchange can continue run at an economic price point comparable to the costs of using Office 365.

Poor network links to the Internet: Sometimes we forget that not every company enjoys high-speed and reliable Internet connections. It might be the case that offices are stuck at the end of an extended hub-and-spoke network that simply needs to be upgraded or it might be that poor connectivity is a fact of life in some or all locations. Office 365 depends on the Internet to connect users to Microsoft datacenters. The exact bandwidth and latency needed depends on the client mix (Outlook creates a heavier demand on the network than OWA does), number of users, and working patterns (always size for peak demand plus contingency). Remember that you also must move mailbox data to Exchange Online, a process that won't be quick if the network lags.

Old desktops: Exchange Online only supports certain versions of Outlook and browsers. Organizations that use software such as Outlook 2003 or older browsers should factor upgrades into the migration. Deploying a new version of Office or a complete desktop refresh is expensive and takes time and attention to detail to ensure that user productivity is not disrupted. The click-to-run version of Office uses streaming and virtualization technology to install the Office desktop products. It is an excellent way of addressing the issue of outdated desktop software as it allows for automatic updates to be downloaded and installed on user PCs. Organizations can configure Office 365 Pro Plus to manage software updates in-house if required.

Recent Exchange upgrade: A company that has recently (in the last two years) upgraded their IT infrastructure for Exchange 2013, probably including a hardware refresh and potentially an upgrade to Windows Server 2012 R2 and other components, might not have the appetite to go through the additional step of moving some workload to Office 365. A similar case can be made for companies who have moved to Exchange 2010. Although the software is now approaching the end of its lifecycle, Exchange 2010 is still a fine email server, and an understandable desire probably exists to extract a reasonable return from the investment put into the upgrade.

Other complexities exist that are not in this list. For instance, any company who is already running on a hosted email service such as a managed service based on on-premises Exchange or a completely different platform like Gmail or SMTP mail will have their own difficulties to overcome.

Now that we understand the various categories of companies that might consider moving to Office 365, let's consider the money question.

The Economic Imperative

On the surface, saving money is an excellent justification to move to the cloud. Many commentators focus on the fixed per-month subscription fee and compare this to the all-in cost (if it is known) to run an in-house system. Salespeople who want to push the virtues of the cloud love to talk about the fixed-price per month, especially if they can get you to focus on the lower cost plans. Once you start thinking that you can buy cloud services for $6/month per user, that impression fixes itself in your mind and a certain view that "the cloud is cheap" forms. It can be very difficult to change this impression, even when you realize that you really need one of the more expensive plans and will pay $20+/month per user.

Invariably the comparison is positive for the cloud because organizations often do not fully understand the complete cost picture are therefore do not factor all the cost elements into the equation. It's true too that the notion of paying a fixed monthly cost is attractive because it allows the company to manage cash flow more precisely than the sometimes-erratic spending patterns of IT. It is also clear that cloud systems are more flexible than in-house systems when the time comes to add or reduce capacity.

Figuring Out Cloud Costs

You will never quite know what the actual cost base for a cloud deployment is until after you complete the deployment phase (migration of users and applications) and operations stabilize. Only then will you know exactly how much the cloud is costing and where those costs lie.

But before you make the decision to embrace the cloud, it is wise to figure out exactly what the current on-premises environment costs. You will need this data to compare against cloud expenditure to show any savings Let's discuss the typical cost buckets that you should consider.

Hardware

Your on-premises deployment probably uses a range of different servers including Active Directory servers, Exchange servers, mail hygiene or bastion servers, SharePoint servers, Skype for Business servers, and administration systems (workstations and servers). Some of these servers might run as virtual machines on a hypervisor (like VMware or Hyper-V). You need to capture details of all the servers involved in the workload to move to the cloud and figure out their annual running cost, including capital depreciation, replacement cost, power consumption, cooling, and other datacenter expenses.

Software

You won't need software licenses for Windows Server and the server applications after you transition their workload into the cloud, but you will need to continue to pay for some servers, especially if you plan to run a hybrid environment. In this case, you'll need to have servers for tasks such as directory synchronization and perhaps single-sign on based on Active Directory Federation Services. You might route your email from the cloud to on-premises servers for delivery, so you'll need servers for that purpose – and those servers must have licenses. Depending on the monitoring framework that you use, you might have to upgrade it to deal with cloud services. It's very important to figure out exactly what portions of the overall workload will remain on-premises because this will enable you to understand what server hardware and software licenses to but, power, license, and run in tandem with your cloud subscriptions.

Every Office 365 user must have a license before they can access the service. To calculate the monthly subscription charge for Office 365, you need to know how many users will need licenses and what plans they use. Remember that shared mailboxes do not need licenses (unless they have archives, are on hold, or use more than a 50 GB quota). Logically, the more feature-rich plans are more expensive, so you need to understand what people need to use and then match those requirements with a suitable Office 365 plan.

Remember to include all on-premises functionality in your calculations and then find what Office 365 plans best match your needs. Standalone Exchange Online and SharePoint Online plans exist for those who do not need the full range of functionality available in a plan like Office 365 E3. Kiosk (web-only) plans exist for "frontline" workers, people who do not have workstations and only need intermittent access to applications like Outlook or OneDrive.

Microsoft inevitability guides customers towards higher-priced Office 365 plans. Apart from increasing Microsoft's cloud revenues, there is good reason for this as customers can access many features in these plans that are unavailable to the lower plans. You must decide whether you need functionality like Cloud App Security, Advanced Threat Management, or Advanced Data Governance to justify buying Office 365 E5, and how many people need such a plan. Another thing to consider is whether it is cheaper to buy a lower-cost plan and then buy add-on components to make specific functionality available to selected users.

Remember that Office 365 does not run in a vacuum and that it depends on other Microsoft technology. Every Office 365 tenant has a basic version of Azure Active Directory, but you will need premium licenses if you want to use certain functionality like policies for group naming and expiration. Many companies buy the Enterprise Mobility and Security suite because it has functionality that they need, like Intune to control mobile devices, as well as premium licenses for Azure Active Directory and Azure Information Protection. The point here is that calculating the cost for Office 365 is not just the sum of monthly plans multiplied by users: the actual cost of what you want (or need) might be higher. Be sure that you understand all the licensing requirements as you build the case for Office 365.

Microsoft Office

You might be quite happy to run the Office 2003 or Office 2007 applications on your desktops. Unfortunately, Office 365 won't take the same view of the world as it needs up-to-date software before it will allow users to connect to its services. If you do need to upgrade, you should consider using Office 365 Pro Plus (click to run) to ensure that the Office desktop applications receive updates automatically over the Internet. Different channels dictate how often users receive Office updates, so some control is available. Office 365 no longer supports Office 2010 and Office 2016 is the default version for Office 365 connectivity.

Applications

Most companies have applications that they have built in-house. These applications range from Visual Basic programs and Excel macros to full-blown database applications. Some of these applications might have dependencies on the workload that you plan to move to the cloud and might therefore need code changes so that they can continue to function afterwards. That is, if you can find the code and have someone available who understands how to make the necessary updates to the code. One major factor to consider is that Office 365 does not allow programmatic access to the data that it manages in the same way that is possible on-premises when you control all the moving parts, so programmers must use APIs such as the REST-based Office 365 APIs to interact with online services. In turn, this might involve some retraining or knowledge acquisition.

Browsers

You might decide that you are going to use browsers to access Office 365 and that web clients suffice. After all, modern web clients are highly functional and support features like offline access. The plan is viable, if users have modern browsers on their PCs, which means Microsoft Edge, Internet Explorer 11, or the latest version of Chrome, Firefox, or Safari (for Macintosh computers). In addition, it is possible that a browser is unable to access specific Office 365 features. For example, only Internet Explorer supports S/MIME encryption with OWA. By contrast, at one time, only Edge and Chrome supported the upload of complete folders to a SharePoint Online or OneDrive for Business library while Internet Explorer could only upload a file at a time. Upgrading a browser on user PCs is a task that varies in difficulty from easy to extremely hard depending on the browser, the number of PCs and the PC management framework that you use. In all cases, you must use a supported browser (see the Office 365 system requirements). And of course, if you update browsers, make sure that the upgrade does not affect other applications. It has been known to happen!

Networks

You won't do anything with Office 365 unless you can access its services, and that means connecting across the Internet to Microsoft's datacenters. You need to understand just what kind of access your company will need to the public Internet to carry the anticipated traffic to Office 365 and all other Internet traffic that your business needs, plus a reasonable uplift for anticipated growth over the next few years (as there is no point in upgrading to a connection that just about copes with Office 365 and runs into problems soon thereafter).

People

Running an on-premises environment needs knowledge and experience of Windows, Exchange, SharePoint, and all the other products that combine to form an enterprise environment. Over time, the people who run IT systems build a certain insight into the company and how it conducts its business. For that reason, I hesitate to say that companies can achieve workforce savings by transitioning workload to the cloud. Perhaps it is possible to save by letting some operations staff go because administrators no longer perform tasks such as server maintenance, but usually you find that other work appears to fill the vacuum left by work now done in the cloud. For example, in a hybrid environment, someone must manage tasks such as directory synchronization, single sign-on, certificates, and mail flow.

Even when Microsoft assumes total responsibility for the management and operation of all the workloads running inside Office 365, someone must administer these applications and manage Office 365 on behalf of the company. User accounts do not create themselves and there are always bits and pieces to keep everything working smoothly. Because the mundane operations involved in server management no longer exist, administrators need fewer hours to manage online applications, but this is not a reason to cut their positions. During the migration period, administrators will have plenty to occupy themselves as workloads move to the cloud. Afterwards, they will have new tasks to perform (such as hybrid management) and can take on new responsibilities such as setting up enterprise voice operations based on Microsoft Teams or creating a document management strategy for the company that exploits SharePoint Online and replaces old Windows file servers with OneDrive for Business. They can investigate new capabilities that the company has never been able to exploit because staff were not available, such as figuring out whether the Outlook app model offers any potential for business-specific solutions. And they can dedicate time to setting up a monitoring framework that deals with both on-premises and cloud components and is available to administrators, support staff, and potentially even users.

Another important role is to stay informed about changes that occur inside Office 365 and associated technologies like Azure Active Directory. Change creates opportunities but also causes challenges for users and operations, so someone needs to check the ongoing changes and assess their impact against company operations. In short, moving to the cloud removes some work while also creating new work. The notion that companies can achieve considerable savings by making IT staff redundant is dubious and often does not stand up when challenged.

Training

It's obvious that a considerable upheaval occurs within a company's technical infrastructure when a move to Office 365 occurs. That upheaval affects users, administrators, support personnel, and managers alike. Users need training to work with new software (like how to find documents with Delve or the proper etiquette for using Teams) and how to recognize and cope with common issues, such as a glitch with Internet connectivity that means they cannot connect to Office 365. If you enable something like multi-factor authentication to augment security or use new features exposed in Office 365 like rights management and message encryption, users need education on these points too.

Administrators need training on the new moving parts that connect your environment with Office 365. If you change your monitoring and reporting framework, they'll need to know about that too. Support personnel like the help desk need to understand how to handle problem tickets when they have no control over a large part of the picture. They need to understand how to work with Microsoft Support, how to figure out whether problems are internal to your infrastructure or caused by Office 365, and how to track progress of problems escalated to Microsoft. Managers, especially IT Directors or CIOs, need to understand how the world of IT is changing and how a decision to embrace something like Office 365 brings its own set of advantages and disadvantages so that they can better guide the progress of the company's IT environment. In a nutshell, lots of change is in the air and will affect people. If you don't train them to cope with the change and how to exploit the new functionality, then you're creating some hurt for users and administrators and won't maximize the potential benefit of moving to the cloud.

Add-on Products

Although Microsoft sells Office 365 as a complete solution, a lot of interesting functionality is also available in add-on products created by Microsoft and third-party ISVs. It is difficult to offer precise guidance on this point because the needs of individual companies vary so much. Examples of areas where you might look for extra functionality include:

- Security, such as an alternate email hygiene service. Microsoft does not recommend that email traffic to Office 365 passes through other hygiene services because they say that this affects the ability of Exchange Online Protection to detect and isolate malware and other threats.
- Monitoring of Office 365 workloads and associates services such as hybrid connections and directory synchronization.
- Reporting and auditing to keep and analyze data for longer than the 90 days made available by Office 365. The retention of audit data for longer than 90 days is important for any company that comes under the scope of the European Union's General Data Protection Regulation (GDPR) as you might need these records to prove or disprove access to personal data.
- Backup of mailboxes, SharePoint Online sites, and other information. Typically, these backups copy data to a cloud datacenter run by a third party. The case for implementing backups outside Office 365 varies for the different workloads. Native data protection and the volume of mailbox data possibly makes off-site backups for Exchange Online less attractive than those for documents and other data held in SharePoint Online and OneDrive for Business. Be aware that major challenges exist in the backup of data belonging to cloud-only Office 365 applications based on Azure data services like Teams and Planner.
- Compliance, for instance, to extend Data Loss Prevention to cover more than Office 365 data.

Creating a Network to Support Cloud Services

As discussed earlier, Office 365 is all about "the cloud". In many respects, this is shorthand for "the Internet." No Office 365 project can succeed without reliable high-speed and high-capacity connectivity to the Internet, so the first and most fundamental question that any company who wants to move from an on-premises infrastructure to use cloud services is can their network infrastructure cope. Given the state of modern communications and the profusion of fiber-powered networks around the world, it is surprising just how many companies discover that they might have difficulty securing enough high-quality bandwidth, but it does happen. In these instances, all you can do is wait for the local network provider to upgrade their pipes.

Organizations that move to Office 365 often discover that their internal network infrastructure is not fit for purpose. This is quite normal and logical. You cannot expect a network design created to serve the needs of an internal infrastructure where servers and clients are co-located on the same WAN to suddenly transform itself to be able to cope with completely different traffic patterns and user demand. Thus, a move to embrace Office 365 is an opportunity to review your network from several perspectives, including:

- Are internal network upgrades necessary to accommodate the volume of client traffic to Office 365 and other Microsoft cloud services? For instance, internal routers, proxy servers, or NAT-routers might not be able to handle the increased load caused by all the TCP/IP sessions consumed by users as they connect to Office 365 services. Project experience shows that a single user can consume up to 20 sessions to connect to Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business, Teams, and other services. To help, Microsoft publishes information about network planning and performance tuning for Office 365. Another page covers network capacity and devices, including elements such as WAN accelerators. Another interesting source of information is the Microsoft Cloud Networking for Enterprise Architects poster. This poster shows some of the changes in an on-premises network that tenants might need to make to support connectivity to Microsoft cloud services.
- What ports and IP ranges must be available through firewalls to allow users to connect to Office 365? To help in this task, Microsoft regularly publishes updates for the URLs and IP address ranges used by Office 365. Over time, Microsoft plans to replace the HTML, XML, and RSS data for network changes with a web service that customers can consult to learn about changes in Office 365 networks, including updates to route traffic to Office 365 and avoid latency and other network challenges.
- Will application-level changes force generate increased demand for network bandwidth and capacity? For instance, both the cloud and desktop Office applications have an AutoSave feature to capture changes made to documents during editing sessions so that users do not have to save files. AutoSave works for documents stored in SharePoint Online and OneDrive for Business sites by creating new versions of the documents to store changes generated during an editing session. The AutoSave activity uses network bandwidth to send the updates from user workstations to Office 365; the OneDrive sync client might then synchronize the updated documents back to workstations by the OneDrive sync client. These changes can generate an added network load that does not exist in on-premises environments.
- Are any changes needed in network security? For example, Office 365 supports multi-factor authentication (MFA). If you deploy MFA to protect Office 365 data, can you use MFA to protect other applications?
- Can you improve data routing within the internal network? For example, to carry traffic from outlying business locations to an Office 365 front-end (point of connection).

Client traffic changes because the target servers are no longer within the internal network. Instead, clients connect via HTTPS to cloud-based servers across the Internet to applications running inside Office 365 or to SQL or other application servers running inside Azure. The outbound links that connect your company to the Internet must be able to support the new workload. The exact type of link needed varies depending on the number of clients that you expect to be active at any time, the type of clients, and the cloud services they will access. Although Microsoft has created a large network of local front-end points of connection for Office 365 (Figure 2-1) to speed traffic to its datacenters, unless the link from your company locations to Microsoft's front-ends can carry the amount of user traffic, users will not be able to work as well as they should.

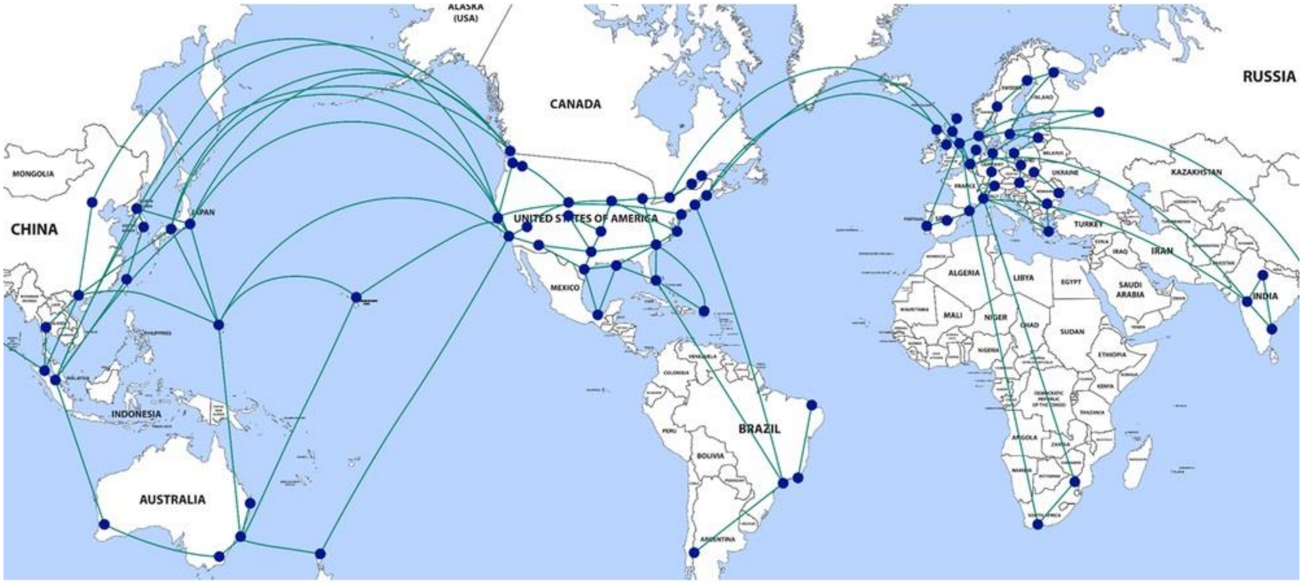

Figure 2-1: Microsoft global network with Office 365 front-end shown (blue dots)

If you run on-premises servers today, you probably have some data to show how much network bandwidth applications and users consume. One rule of thumb is to double (some say triple) this figure and use that amount as the basis for planning. Advice and guidance on this topic evolves over time as Office 365 changes and knowledge increases, so it is best to ask Microsoft or an experienced consulting company for their recommendation as to the capacity you need – and to then add 30% or so to cater for growth in user demand and to accommodate new applications and features used within Office 365. Because Office 365 evolves over time through the introduction of new applications and features, usage patterns and consumption will change too. It is therefore important to keep an eye on changing demand over time.

Remember that moving to Office 365 will not make a bad internal network any better. In fact, the extra demand that the added functionality available in Office 365 might generate when users realize that it exists is likely to put increase pressure on the internal network. If that network is barely able to cope with the demands of on-premises client-server connections, it will do no better and is likely to do worse when cloud services take over.

Before beginning to migrate to Office 365, it is sensible to upgrade your external links so that they can handle the new load. You can start the migration using existing network capacity, but you might find that the migration activity interferes with other work, such as access to external web sites. In addition, as you move users to the cloud, those users will want to access their new cloud-based mailboxes and other applications like Teams. They will quickly become unhappy if cloud access is slow and unreliable because they hit problems like port exhaustion due to lack of publicly routable IP addresses (see this support article). In addition, if your organization uses central connections to the Internet, you will probably find that a separate link per location delivers better results. A slow or constricted connection to the Internet is not a good foundation for success with Office 365. If your connection cannot cope with the traffic to the cloud, your Office 365 project will die a quick death.

Although an expensive option, it is possible to implement a dedicated network connection to Office 365, such as Microsoft’s Azure ExpressRoute for Office 365 service. ExpressRoute uses a dedicated MPLS connection between your datacenter and Microsoft's network to ensure that traffic flows as if it were on your internal network. In general, Microsoft believes that careful management of an internet connection is enough to deliver the necessary connectivity to Office 365, especially now that their network of local connection points is so extensive. Before you can use ExpressRoute, Microsoft must assess your network to decide whether ExpressRoute will achieve a measurable improvement in connectivity. One scenario where ExpressRoute might help is where many people in a single location use the Microsoft Phone System because ExpressRoute can prioritize voice traffic over other traffic.

When you plan for new network capacity, make sure that you accommodate three types of traffic:

- User connections to the new cloud environment plus existing work. Remember that users often make use of company networks to access external social sites such as Facebook and Twitter during work hours. You can try to restrict this access but, in many cases, this is like pushing water uphill, so it is best to include a certain overhead for personal network activity. Remember too that different clients have different network characteristics. For example, Outlook clients consume more bandwidth than OWA, especially if you use add-ins that need network access. As explained in Chapter 16, voice and video conversations are sensitive to network conditions and need certain basic capabilities to be able to function. New applications such as Teams introduce new demands on the network. Still another thing to consider is the increased demand for mobile access to data. Office 365 has mobile clients for most applications and the increased use of mobile clients inside company offices might affect Wi-Fi networks if those networks cannot deal with the number of connections and the bandwidth demand. Microsoft has network calculators for Teams, Skype for Business, and Exchange that help assess likely demand (further information is available here).
- Migration of user data to the cloud. Moving 500 users might happen in a cutover operation during one weekend. Migrating 50,000 users will probably take a little longer. In both cases, you still must move mailbox data from servers in your internal network across the Internet to an Office 365 datacenter. Depending on how much data is involved and the available throughput from your network to Microsoft, that movement could take longer than you think.
- Administration operations. Intelligent applications like Outlook isolate users from the effect of network outages and allow them to work offline. However, all Office 365 administrative operations occur online and a reliable (and fast) network connection is necessary if you want to be sure that administration can be performed without difficulty.

Information presented by the Office 365 product group at the Ignite 2017 conference gives advice about:

- Strategy.
- Planning.
- Implementation.

These sessions are valuable in terms of framing the discussion about how your network infrastructure might have to change to protect the Office 365 user experience. Another interesting document is a Microsoft IT report outlining some of the network challenges they faced in moving Microsoft users to Office 365. While your company might not be the size of Microsoft, there is usually something to learn from descriptions of how other companies dealt with technical issues. Finally, the top ten troubleshooting tops for Office 365 network connectivity is a useful document to consult if you run into problems.

During the migration period, the volume of network traffic will be higher than normal because of the need to move information like mailbox data and documents to the cloud. After the migration period is over, network demand should settle into a more predictable load. There will be peaks and valleys in demand, but you should be soon well acquainted with the general shape of network demand for different locations and be able to make whatever changes are necessary.

Executive Buy-in and Communications

Few major projects succeed without executive buy-in and support. A good communication plan to explain why the project exists and the benefits expected to accrue to both the company and employees is also important to offset the upheaval that will probably be encountered as mailboxes are migrated, networks change, and clients are updated.

Executives should focus on simple messages like:

- We are buying the best-of-breed Office software from Microsoft.

- Using Office 365 will allow the company to be more flexible and adaptive to changing business circumstances.
- Employees who worked on our previous messaging systems will now work on more important projects such as figuring out the corporate strategy for using SharePoint Online, making better use of Skype for Business Online (perhaps as a replacement for a traditional PBX), or determining whether Office 365 Groups or Yammer is the most suitable collaboration platform for the business.
- Moving to the cloud is a safe and secure choice.

The communication plan will cover:

- A summary of what's happening – the company is upgrading and improving its email and collaborative capabilities by moving to Office 365.
- When the changeover will occur and when employee mailboxes will be migrated.
- The functionality changes and improvements that users will see and how these updates will make work easier. Some simple scenarios might be included, such as how to set up a group mailbox to support project teams.
- Tips and techniques for making a smooth changeover.
- Anything an employee must do to enable connectivity with Office 365. For instance, those running older versions of Outlook or old browsers might have to upgrade their software.

Every company is different, and the suggestions outlined above are merely the start of the discussion about how to lead people through change.

Dipping Your Feet into The Water

Even after doing extensive research to verify whether Office 365 is the right platform for your company, there is nothing quite like getting your hands dirty to make a technologist happier with a technology. Office 365 makes test drives easy by allowing you to sign up for a 30-day free trial. Essentially, you can create a fully functional test tenant and use it for 30 days to decide whether Office 365 works for your company. And if you’re still not sure about Office 365 after that period, you can simply discard the original trial, extend the trail, or start off again with a new tenant.

Using a trial tenant as a proof of concept is a great way to get a sense of how Office 365 works in practice. The exercise will not expose some of the more complicated challenges, such as how to migrate public folder data or how hybrid connections or single-sign on work over an extended period. However, the information gained from a trial is certainly enough to gain a broad understanding of the different parts of the service and how the administrative experience differs from your on-premises environment. You’ll be able to figure out how to move workload to the cloud and what extra functionality exists – or where functionality gaps exist because something like a third-party add-on is unavailable within Office 365.

Some companies start off with a trial tenant and then convert the trial into a paid-for service after the 30 days. This is OK if you plan for the eventuality and go ahead on that basis. However, you should be aware that no functionality exists inside Office 365 to transfer data from one tenant to another. Third-party tools are available, but these come at added cost.

You also need to make sure that any settings used to direct email to the trial tenant such as validated domains are removed afterwards. All-in-all, it is usually a better idea to regard a trial tenant as no more than a test and to accept that if the company decides to embrace the cloud, you will start over from scratch and use a new tenant.

Office 365 Partners

Microsoft promises free onboarding aid to Office 365 for companies who buy more than 50 seats and will provide some funding to accredited partners to help with migrations. The funding available through FastTrack can be very helpful to offset the overall cost of a migration. However, FastTrack migrations are very structured and follows a strict playbook. It might or might not be enough for the needs of a small company that wants to move from on-premises Exchange to Office 365, but it is unlikely to be enough for complicated migrations. This is when you might need to either run the migration using internal resources or seek the help of a Microsoft partner who specializes in Office 365.

Given enough time to acquire knowledge and run some trial migrations, it is possible for any experienced Exchange administrator to prepare an Office 365 domain and move mailboxes to it. The steps needed to configure hybrid connectivity are largely automated and well understood so that attention to detail and good preparation will get most administrators through the process. Of course, there are always examples of situations that are unique in certain aspects, such as migration projects that propose to collapse several Exchange on-premises organizations into one Office 365 tenant, but in general the migration of a normal Exchange setup composed of a single organization based on a single Active Directory forest is usually straightforward. Outside of moving mailboxes, the kind of detail that causes problems include single sign-on (SSO), federation, mail routing, message hygiene, and hybrid co-existence. We discuss issues linked with migration the companion volume.

Given that email servers must continue running while work proceeds to prepare for migration, you might need to engage some outside help to make the project happen in a reasonable period. The options are to use:

- Microsoft Consulting Services (MCS).
- A Microsoft partner specializing in Office 365, including the consulting and support arms of major IT companies.

Although expensive, MCS has the advantage of being part of Microsoft and offers the reassurance of being a single throat to choke if anything goes wrong. On the other hand, an independent partner often offers a more realistic opinion about how to run successful projects and the likely pitfalls that exist along the way. In addition, independent partners often have deep knowledge of third-party solutions that can help solve some of the more complex situations that occur in migration projects.

Microsoft partners exist in every market. In selecting a partner, consider the following questions:

- Is the partner a member of the Microsoft Partner Network? A partner who is not a member misses out on many important resources and tools that Microsoft makes available through its network.
- How many Microsoft accredited specialists does the partner have on staff, how recent are the accreditations, and in what technical disciplines do their people have experience and knowledge? Non-Microsoft accreditations such as CISSP (security) might also be useful, depending on the areas covered in the project. Partners who hold silver or gold competency levels for Office 365 can receive FastTrack funds to help in migration projects.
- Remember that accreditation and certification is one thing. Being able to do a job is quite another (the IT industry is littered with certified individuals who are incapable of doing any useful work). Ask about the experience the partner and its staff have with Office 365 and what projects with similar requirements have they been successful with in the past.
- Ask about the roles played in the projects by the people that the partner proposes to involve in your project.
- What areas of specialization does the partner cover within Office 365? A partner who specializes in Skype for Business, SharePoint, or Yammer is probably not a good choice for companies who want to migrate Exchange 2010 to Exchange Online, especially when you throw the intricacies of hybrid

connectivity and directory synchronization into the mix. On the other hand, if your focus is on moving workload from SharePoint on-premises to SharePoint Online, experience with Exchange will not be much help. Introducing Delve often needs a reasonable amount of SharePoint knowledge because of the way that Delve can "uncover" poor sharing and access control practices.

- Some parts of Office 365 are relatively new. These include Office 365 Groups, Planner, and Teams. If you are interested in these areas of functionality, you need to find out whether the potential partner has relevant experience of deploying, managing, and troubleshooting these components.
- The deployment of the Microsoft Phone System often needs experience with voice systems, especially when the need arises to replace traditional PBXes.
- The deployment of high-end features such as Office 365 Cloud App Security, Advanced eDiscovery, and MyAnalytics also usually needs specific experience in these areas.
- The world of application development is different inside Office 365. New tools like Flow and PowerApps do not exist in the on-premises world and new APIs like the Microsoft Graph are available to expose more data to applications than ever before. If you need to write some code, look for people who have knowledge of the new tools and APIs before you decide on your partner.
- Do not forget that Office 365 is at the center of an ecosystem. Microsoft does not have solutions to every possible feature request or customer need and it is good to find a partner who has knowledge of solutions to areas such as service monitoring and reporting, security, external archiving, backup, and so on.
- How skilled is the partner at understanding how to exploit the Office 365 plans, add-ons, Azure Active Directory, Azure Information Protection, and Enterprise Mobility and Security to meet the needs of your company?

Specifically, when considering the migration of workload from Exchange on-premises servers to Exchange Online, ask:

- The experience they have with on-premises Exchange, specifically the version you run. Although they share some characteristics, Exchange 2010 is very different to Exchange 2016.
- Their knowledge of various aspects of Exchange that you might want to use when you move to the cloud, such as encrypted email, different email clients, public folders, and so on.
- Their experience with other areas associated with Exchange such as Exchange Online Protection, Azure Active Directory, rights management and encryption, etc.

Apart from these points, you might also ask what contribution the partner makes to the local technical community, how useful their web site or blog is in terms of the information that you find there, and whether any of their personnel are Microsoft Office Servers and Services 365 MVPs as they have background channels to the development group that might be useful in resolving problems that arise during the project.

The Value of Hybrid Connectivity

Microsoft has done a lot of heavy engineering to create hybrid connectivity for Exchange. In some respects, they had to do this work to preserve the Exchange installed base. After all, most large companies will not countenance the "all in" approach to the cloud as it is the nature of enterprise IT to move into new areas quite slowly after due diligence is done to identify issues that must be solved before full implementation can proceed. Setting up a hybrid connection between on-premises Exchange and Office 365 allows these companies to dip their toe into the cloud (a mixed metaphor) by creating the links to enable interoperability between the two platforms. Some workload can then be transferred to the cloud, the results observed, and a decision made as to the best way to proceed. In some cases, the decision will be to move more workload, and perhaps even to proceed along the line so that most mailboxes are transferred. In others, the decision will be to retain a substantial portion of work on-premises and use Office 365 for tactical purposes, such to support mailboxes for specific types of employees. The transfer of workload follows the pace set by the company and could extend out over many years.

Without hybrid connectivity, Microsoft would offer the same one-way trip to the cloud as Google does when it proposes to migrate workload to Google Apps for Work. If no possibility exists to run on-premises and cloud platforms together as a single environment, customers who want to move to the cloud would have to plan on an accelerated transfer, much like the switchover approach used to move smaller companies to Office 365. This is a perfectly acceptable technique when dealing with a relatively small number of users, mailboxes, and data; it is less satisfactory when the numbers mount up. Other complicating factors that make it harder to plan for a fast switchover include the distribution of users across multiple company locations, especially when international employees are involved.

Of course, it's possible to extend a switchover period without hybrid connectivity by relying on SMTP to keep everyone connected. Although this approach works, it means that you must operate two totally isolated environments until the final mailbox is moved into the cloud. That might be easy in some circumstances, but issues such as single sign-on, mailbox delegation, calendar sharing, public folders access, and so on tend to complicate matters in most companies who have operated Exchange for a reasonable period.

Hybrid connectivity smoothens the issues by enabling connectivity between the two platforms. It's not a total panacea as some manual interventions are necessary to close the gaps, like the need to manually export and import retention policies and tags to ensure that the same compliance regime exists in both platforms. However, these interventions need a lot less effort than would otherwise be necessary to move to the cloud without a hybrid connection.

As explained in Chapter 8, hybrid connections are also supported for SharePoint. These configurations are less popular than hybrid Exchange, but it's certainly an option to consider, especially if your on-premises SharePoint configuration includes applications or other customizations that cannot run in the cloud.

Hybrid connectivity also gives customers a "plan B" if moving to the cloud does not deliver the advantages expected when the decision was made to use Office 365. The same facilities that allow mailboxes to be moved from on-premises to Exchange Online can be used to move mailboxes back to Exchange on-premises. Again, some gaps exist – like how to move public folders back because the public folder migration tools run in one direction – but overall, hybrid connections are two-way and can therefore be regarded as a way to reduce dependency on Office 365 should the need arise.

The Need for Plan B

No CIO wants to implement a new platform without knowing what will happen if things go wrong. All projects carry a certain element of risk and a project to move workload to Office 365 is no different. Good planning, solid project management, and technical expertise all mitigate the risk, but some cloud projects will end up at a point where management decides that on-premises is the better option. You must then figure out how to move content back from the cloud platform and resume operations on-premises.

Thanks to the engineering investment made by Microsoft to enable hybrid connectivity, Exchange is the easiest application to move back on-premises. Mailboxes can be transferred back to on-premises servers as easily as they can move to the cloud. The only downside is the amount of storage that might have to be deployed to accept inbound mailboxes because users might have become accustomed to the liberal mailbox policies used within Office 365. Another complication is how to deal with content stored in inactive mailboxes; it is easy to overlook these mailboxes because they do not show up in all administrative interfaces and reports.

Mailboxes are relatively easy but everything else is hard. If you have elected to use Azure Information Protection (Chapter 24) to protect information inside Office 365, you might find that it is difficult to access protected content moved back on-premises because it is no longer possible to decrypt that content. A hybrid configuration will help if you keep a connection to the Azure Information Protection service.

You must make sure that you move any customization made to Exchange Online back on-premises so that things like PowerShell scripts, transport rules, Data Loss Prevention rules, retention policies and tags, and so on are moved across. Again, if you are in a hybrid environment these settings should already be duplicated to ensure that the cloud and on-premises platforms remain in tandem, but there's work to be done to make sure that everything is synchronized.

For instance, if you make a big commitment to Teams as a collaboration platform with or without voice integration, what do you do if things do not work out in the cloud and you decide that the best course is to revert to on-premises? You can move voice communications to Skype for Business Server and documents back to SharePoint Server, but the conversations and chat part of Teams is cloud-only. Much of Office 365 is now unique to the cloud platform and no tools exist to move data to a form that is consumable by an on-premises application.

You can synchronize Office 365 Groups to hybrid on-premises environments, where they show up as standard email distribution groups. However, Office 365 Groups do not exist in on-premises software (as is the case for other some user-centric features of Office 365 like MyAnalytics). It is hard to know how to retrieve the information in group conversations, shared notebooks, and document libraries because no export utilities exist, so again this will probably need a great deal of manual effort to recover data from the cloud. Planner adds its plan metadata to the mix of data that you might need to recover to reassemble plans into a reusable state. The same is true for the data used by Microsoft Teams.

Microsoft makes it clear that tenants continue to own their data stored in Office 365:

"*You own your data and retain all rights, title, and interest in the data you store with Office 365.*"

Although it is straightforward to consider the movement of basic data from Office 365 to other platforms, no obvious way exists to move the complete spectrum of data contained within a tenant. For instance, you can copy documents from a SharePoint library to your PC, but how feasible is this approach to capture the complete corpus of information existing in SharePoint and OneDrive for Business sites within a tenant? That information includes lists, document libraries, OneDrive for Business sites, and eDiscovery cases.

The Office 365 Video portal is another challenge. This is an application that allows tenants to set up a kind of "Internal YouTube" for the company through channels that categorize videos for viewing inside the company. The video portal is based on an integration between SharePoint Online and Azure Media Services. The portal is good at ingesting content but does not have the same kind of export functions, which poses an issue should you need to recover the video content and metadata at some point. And if you use Sway, you need a way to recover its files too.

Third-party software vendors offer utilities to help move content to Office 365, but the same capabilities do not exist to move information out of Office 365 back to on-premises servers. Given current trends to move away from on-premises servers, this situation is natural as it would take a bold decision to create a migration tool to move content from the cloud.

Well-planned migrations usually proceed to plan and are successful. Most Office 365 migrations are, not least because of the expertise available to assist companies in the transition. But wisdom and prudence dictates that you should always have a Plan B – at least in outline – just in case your project experiences problems.

Cancelling a Tenant Subscription

Office 365 is obviously a commercial business and Microsoft is quite happy to keep your data online while you continue paying the monthly subscription fees. If a license is removed from a user account, its data stays accessible for 30 days and is then removed. The exception is when a mailbox is put on hold before the account is deleted. In this case, the mailbox is regarded as "inactive" and is retained while the hold remains in force (see Chapter 6 for more information).

However, you might decide that Office 365 is not for you and go ahead and cancel a tenant's subscription. Hopefully, you will have carefully considered this decision in advance and put steps to recover all the information that exists in the different Office 365 applications. After a tenant subscription is cancelled, a formal lifecycle process begins that eventually results in the complete and permanent removal of all tenant data from Office 365. Table 2-4 lists the steps in the tenant removal process. For more information, see Microsoft's online documentation.

Period	***Subscription Status***	***Effect on data***
1-30 days	Expired	Users will see warnings about losing access but can continue accessing their accounts and work with data.
31-120 days	Disabled	Only global or billing administrator accounts can access the tenant for the purposes of either recovering data or to reactivate the tenant
After 120 days	Deprovisioned	An automated process starts to systemically remove all tenant data, including inactive mailboxes and any others that were on hold.
Within 3 days of ending subscription	Expedited deprovisioning	Upon customer request, the process to remove tenant data can be expedited to ensure that all data is removed within three days of the request.

Table 2-4: When tenant data is removed from Office 365

Note that the processes that remove tenant data after 120 days are constrained by resource availability. The data might therefore be removed after 120 days, 121 days, or soon thereafter. If you need the data to be removed sooner, you must ask Microsoft to start the expedited deprovisioning process by filing a support request. To confirm that expedited removal should go ahead, Microsoft support gives the tenant a lockout code that the tenant must input to the Office 365 Admin Center. After the code is entered, the data will be removed from Office 365 within three days. It is critical to understand that once the data is removed it can no longer be recovered or reactivated.

Cancelling an Office 365 installation is a big step. The responsibility for the decision and what happens afterwards stays with the customer, who can decide to let the cancellation process play out or reactivate the subscription within the 120-day grace period.

The case of the annoying prompts: One thing that you are bound to notice after you cancel a subscription or a trial subscription comes to an end is the number of annoying and persistent prompts Office 365 throws up to inform administrators (or anyone who's listening) that a subscription has ended or expired and some data might be lost. And, of course, that all will be well if you would only buy the subscription now. The bad news is that there is no way to suppress these notifications. You must wait until the countdown period (normally 30 days) expires and the subscription disappears – or file a support ticket with Microsoft to ask them to eradicate the prompts.

The good news is that these notifications do serve a valid purpose in that they stop people forgetting that data might be lost. It would be terrible if you overlooked a notification and ended up by losing some important data. Overall, it's best that the notifications are there, even if they are dreadfully annoying when you know that the subscription is unwanted for good reason.

Identities

Before plunging into the intricacies of moving anything to Office 365, we should pause to consider some important questions such as how people are identified within Office 365, how do they authenticate to the cloud to access services, and the knotty topics of directory synchronization and federation. Fortunately, Chapter 3 has answers to many of these issues, so that is our next destination.