IDC PERSPECTIVE

Microsoft's Office 365 Data Protection Strategy: Ignoring Backup and Recovery is Risky for Resilience, Continuity, and Productivity

Archana Venkatraman

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Microsoft's Office 365 Data Protection Strategy

This IDC Perspective discusses Microsoft's Office 365 (O365) data protection strategy. Usage of Office 365 is proliferating as enterprises are rapidly adopting software-as-a-service (SaaS)-based productivity and collaboration tools to ensure productivity, digital resiliency, and business continuity in the post-COVID-19 era. This makes Office 365 central for a business and that means ensuring data protection of O365 is imperative for security, compliance and recovery. A lack of dedicated O365 backup and recovery plan is a risky data strategy.

Key Takeaways

- O365 (or Microsoft 365) is much more than emails, with users accelerating their adoption of Teams, SharePoint, OneNote, and OneDrive, among others. Growing usage of O365 products means growing data footprint in the SaaS environment.
- Only 23% of the organizations IDC surveyed admit to using dedicated third-party backup for their O365 environments. Digitally advanced companies are more likely to have dedicated O365 data protection compared with digital followers.
- Without a dedicated data protection strategy, organizations are exposing themselves to risks such as ransomware; accidental deletion of data and other means of data loss, compliance, and retention loopholes; and SaaS lock-in.

Recommended Actions

- When adopting cloud services, organizations need to fully understand the "Shared Responsibility Model."
- Make O365 backup a key priority to maintain resiliency and business continuity.
- Leverage SaaS provider's native capabilities and infrastructure-level security. But remember to enhance this foundation with third-party data protection architecture to de-risk the SaaS adoption.
- Ensure enterprise-grade data protection strategy covers data across fragmented IT estate including on-premises, multicloud, SaaS, and platform-as-a-service (PaaS) environments.

Source: IDC, 2020

December 2020, IDC #EUR147031720

SITUATION OVERVIEW

SaaS applications such as Microsoft 365 (and previous versions of Office 365) are considered fundamental for modernizing employee experience, introducing new means of collaboration, and creating a digital workplace architecture. SaaS-based email and collaboration have been particularly popular in the COVID-19 remote working environment. According to Microsoft's latest financial results (1Q21), its cloud businesses fueled fast revenue growth in the quarter. In particular, its Office 365 commercial revenue grew 21%.

According to IDC's latest end user survey, more than 77% of organizations said they use Microsoft Office 365. In fact, as many as 90% of organizations in mature economies such as the U.K. use O365, according to IDC's *European Software Survey* in November 2020.

O365: More than just eMails

The Microsoft Office environment includes many productivity and collaboration applications such as Microsoft Exchange, Teams, OneDrive, OneNote, and SharePoint. Teams is fast becoming a key tool to enable remote collaboration, with more than 115 million people using Teams every day (according to a Microsoft blog published on November 16, 2020). Businesses are looking to use the Teams environment as a platform to create business-specific apps and services.

Microsoft itself is putting Teams at the center of O365 innovation and enhancing it by:

- Bringing Power Platform closer to the Teams environment
- Enabling users to create, share, and track data directly within Teams
- Enabling developers with tools (such as the Microsoft Teams Toolkit for Visual Studio and Visual Studio Code) to kick off their Teams app development.

Teams is everywhere. As per Microsoft's 4Q20 financial report, more than 1,800 organizations have more than 10,000 users of Teams and more than 70 organizations have more than 100,000 users of Teams. A vertical intensifying the use of Teams is healthcare. For example, the NHS in the U.K. chose Microsoft 365 to empower its 1.2 million employees with the latest productivity and collaboration tools to deliver better patient outcomes. In addition, the Microsoft 365 E5 user base more than doubled year over year.

As the use of O365 grows, so does the data footprint in the environment.

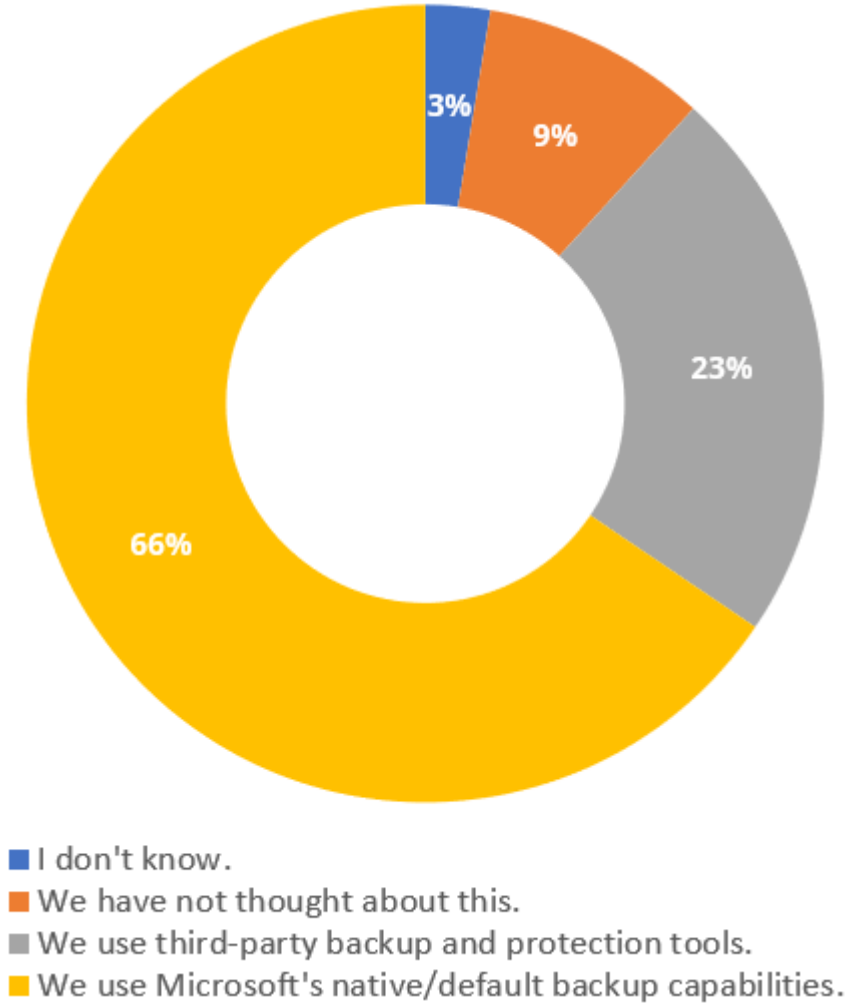
Dedicated Data Protection Still an Afterthought

While O365 is fast becoming the center of business productivity, data protection strategy for O365 environment is still an afterthought, as shown in Figure 2.

FIGURE 2

European Organizations' O365 Data Protection Strategies

Q. How does your organization protect, retain, and recover data in O365 environments (Exchange, SharePoint, OneDrive, Teams, etc.)?



Source: IDC's *European Software Survey*, November 2020 (n = 634)

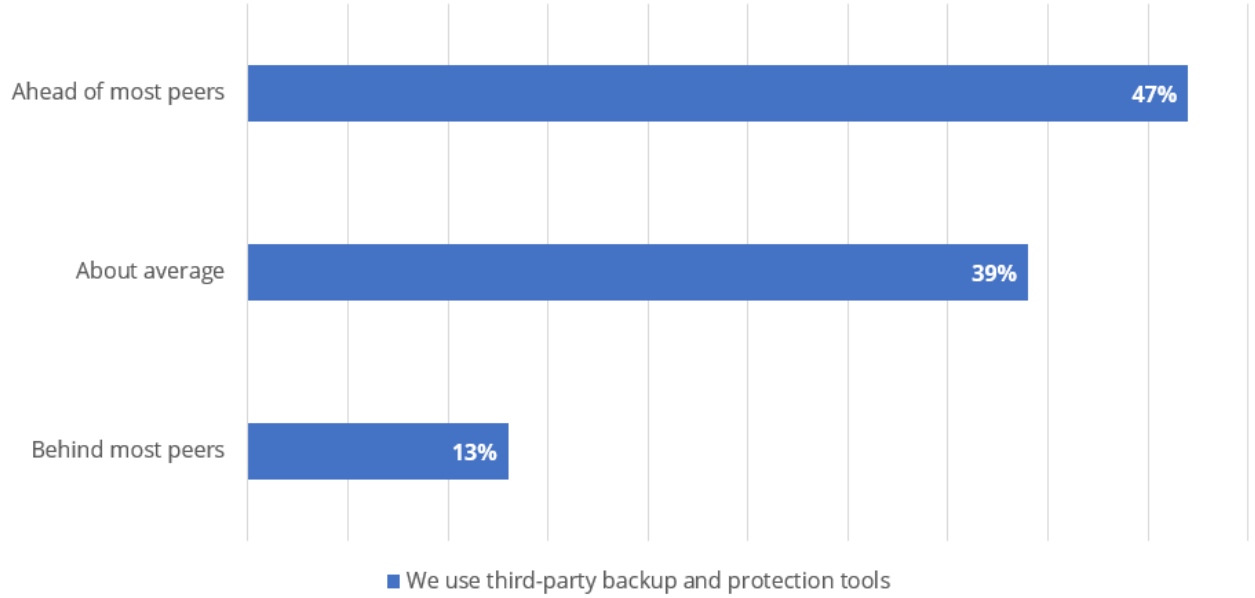
Survey results show that:

- Only 23% of organizations IDC surveyed use dedicated third-party backup and recovery service to protect their O365/M365 environments.
- 77% of M365 and O365 users rely on native capabilities or have not considered data protection for their cloud-based email and collaboration environment.

Digitally advanced organizations are more likely to use dedicated SaaS data protection technologies to ensure business continuity and data recovery compared with those that were less mature in their digital transformation activities, as shown in Figure 3.

FIGURE 3

Use of Dedicated Data Protection Services: Digital Leaders Versus Digital Followers



Source: IDC's *European Software Survey*, November 2020 (n = 634)

Among verticals, only respondents in banking and insurance, telco, and service provider sectors have robust data protection strategies for their O365 and M365 environments.

ADVICE FOR THE TECHNOLOGY BUYER

Microsoft continuously enhances the features and security in its O365 environments. For instance, it has added new capabilities such as Microsoft Endpoint Data Loss Prevention (DLP) to make it easier to prevent data loss on endpoints. It has also added features to better manage DLP alerts. There are also continuous improvements in uptime SLAs, consistency, and availability.

IDC believes that native backup features and default retention in O365 are good starting points, but they are not enough for all compliance and business continuity needs.

However, the real danger is that many organizations believe that native capabilities give them all the data protection they need. In conversations with O365 users, IDC observes that many users confuse Microsoft's availability service-level agreements (SLAs) to backup strategies, while others don't see the need to think of backup for cloud because it is a "different" technology.

Adopting O365 Without Enterprise-Grade Backup Is Risky

Regardless of whether the data is on premises or in cloud infrastructure/SaaS (such as O365), the responsibility of data protection lies with the customer or the data owner – you.

The Shared Responsibility Model

Organizations adopting public cloud services need to fully understand the "Shared Responsibility Model," whichoutlines the division of responsibility between a cloud provider (data processor) and cloud user (data controller).

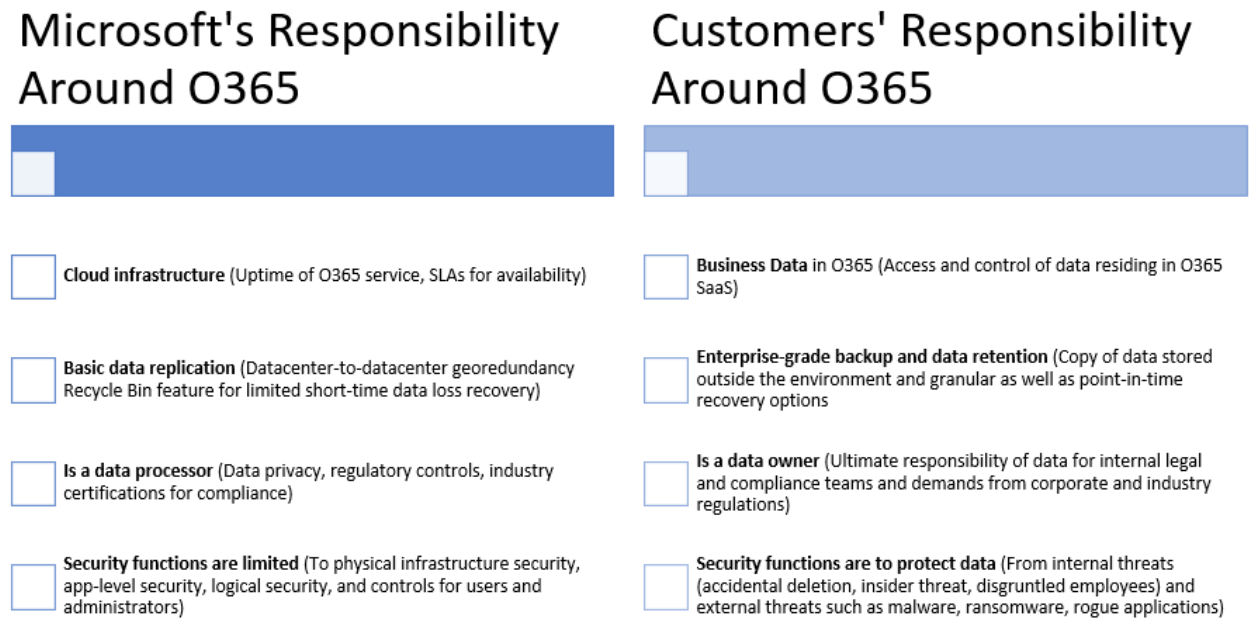
FIGURE 4

The Shared Responsibility Model in SaaS, PaaS, IaaS, and On-Premises Environments

Source: Microsoft, 2020

FIGURE 5

Microsoft Office 365 Vendor-Customer Shared Responsibility Model at a Glance



Source: IDC, 2020

Cloud Provider Guidelines and Best Practice Tips

Microsoft's service agreement recommends third-party backup and recovery. Under Service Availability section 6b, the vendor states that:

> We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages. In the event of an outage or disruption to the Service, you may temporarily not be able to retrieve Your Content. We recommend that you regularly back up Your Content and Data that you store on the Services or store using Third-Party Apps and Services.

Native eDiscovery and Legal Hold Functionality in M365 not Equivalent to Backup and Recovery

Microsoft 365's legal hold capabilities are robust, but they are not fully fit to replace a backup and recovery strategy. For example, in conversations with IDC, customers highlighted the need to have quick data access and recovery to comply with ediscovery needs. They need to consider the cost and IT overheads to recovering specific data in different formats, speeds, and devices. Relying on native legal hold functionality can be restrictive because it cannot help in recovering data that has been accidentally deleted or ensure bulk recovery at speed. Dedicated data protection that covers all data management, including SaaS data, can help organizations in comprehensive legal hold support because they can collect data across enterprise workloads, including O365 data, and keep costs in check.

Exposure to Risks

Given Microsoft's responsibility and supporting technology focus on infrastructure, logical security, and availability, organizations expose themselves to the following risks if they are without third-party backup plans:

- **Data loss, accidental deletion, and security breaches.** O365 is no exception to security breaches — it is vulnerable to internal threats (e.g., accidental deletion of data, actions by disgruntled employees, or access from ex-employees) and external threats (e.g., malware or ransomware). In IDC's *European Multicloud Survey*, 2020, customers indicated ransomware, spiraling costs, and SaaS data protection as the top data protection challenges.
- **Retention and regulatory compliance exposures.** Microsoft offers a 90-day retention policy that does not meet the more stringent data retention regulations for certain industries such as financial services, healthcare, retail, and government. Having a third-party backup can help organizations set their own retention policies based on their business needs and remain compliant with European data regulations.
- **Lack of data control in hybrid deployments.** Full oversight and control of data is a boardroom priority and a first step toward becoming data driven. Without backup, organizations do not have an exit strategy or freedom from SaaS concentration risks.

ADVICE FOR THE TECHNOLOGY BUYER

Without extending data protection to SaaS environments such as M365 or O365, enterprises are exposing data to compliance issues, data loss, security vulnerabilities, and business continuity risks.

Backup for fast-growing SaaS such as O365 is no longer an option — it is imperative for security and data control.

Most data protection vendors offer backup and recovery for O365 environments and are continuously adding more O365 services to their backup repertoires. When investing, organizations must ensure that the backup solution they choose offers:

- **Flexibility and choice.** The business should have the freedom to use existing on-premises capacity or cloud backup targets for O365.
- **Enterprise-grade features.** It should provide incremental backups, granular recovery, automation, and policy-based retention capabilities.

- **Breadth of service.** The solution should be capable of protecting a wide range of M365 environments including emails, Teams, SharePoint, etc.
- **Complementarity to O365.** It should have deep integration with O365 and the customer's existing data protection environment.
- **Innovation.** There should be additional security features such as access control, SaaS usage metrics, and multifactor authentication for additional security.
- **Scale.** The backup solution must be able to scale up or down without capex as business and data demand changes and as SaaS is rolled out more widely within a company.

LEARN MORE

Related Research

- *Western Europe Public Cloud IaaS Storage Market Forecast, 2019-2024: The COVID-19 Pandemic Keeps IaaS Storage Investments Resilient* (IDC #EUR146999320, November 2020)
- *Commvault Brings Metallic SaaS Data Protection to Europe Amid Growing Demand for Cloud-Based Backup* (IDC #IcEUR146988220, November 2020)
- *IDC FutureScape: Worldwide Data and Analytics 2021 Predictions* (IDC #US46920420, October 2020)

Synopsis

This IDC Perspective discusses Microsoft's Office 365 data protection strategy. The adoption of SaaS applications, particularly Microsoft Office 365, is accelerating and its usage expands beyond Exchange to more services such as SharePoint, OneDrive, and Teams to enable productivity and collaboration in the post-pandemic era.

"Despite O365 becoming the center of business productivity, a backup and recovery strategy is an afterthought. Fewer than a quarter of O365 users have dedicated third-party data protection for O365. As data footprint in O365 environment proliferates, businesses need to realise that regardless of where the data is, it is the user's responsibility to protect it," said Archana Venkatraman, associate research director, IDC European Datacenter. "Without a dedicated backup and recovery strategy, enterprises are exposing O365 data to risks such as ransomware, data deletion, and compliance exposures, hindering their resiliency and business continuity."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com