ZONES
First Choice for IT™

WHY A BACKUP STRATEGY IS ESSENTIAL FOR MICROSOFT OFFICE 365

for Security, Compliance, and Business Continuity

Risks without a backup plan.

Microsoft's Office 365 suite of products is an essential piece of the modern workforce. However, its importance also makes it a particularly vulnerable point in most companies' software portfolio. Given Microsoft’s responsibility and supporting technology is limited to infrastructure levels, organizations are exposing themselves to the unnecessary risks if they are without third-party backup plans:

1.

Data Loss & Security Breach

a. No software is immune to security breaches; O365 is no exceptiont

b. Almost half (49%) of all organizations have suffered from an unrecoverable data event in the past three years

2.

Compliance Exposure

a. O365’s default retention policy doesn’t meet regulations for certain industries

b. Industries such as financial services, healthcare, retail, and government are particularly at risk

3.

Lack of Data Control

a. Data control is the first step toward becoming data-driven

b. Without backup, organizations do not have an exit strategy or freedom from SaaS lock-in

Risks without a backup plan.

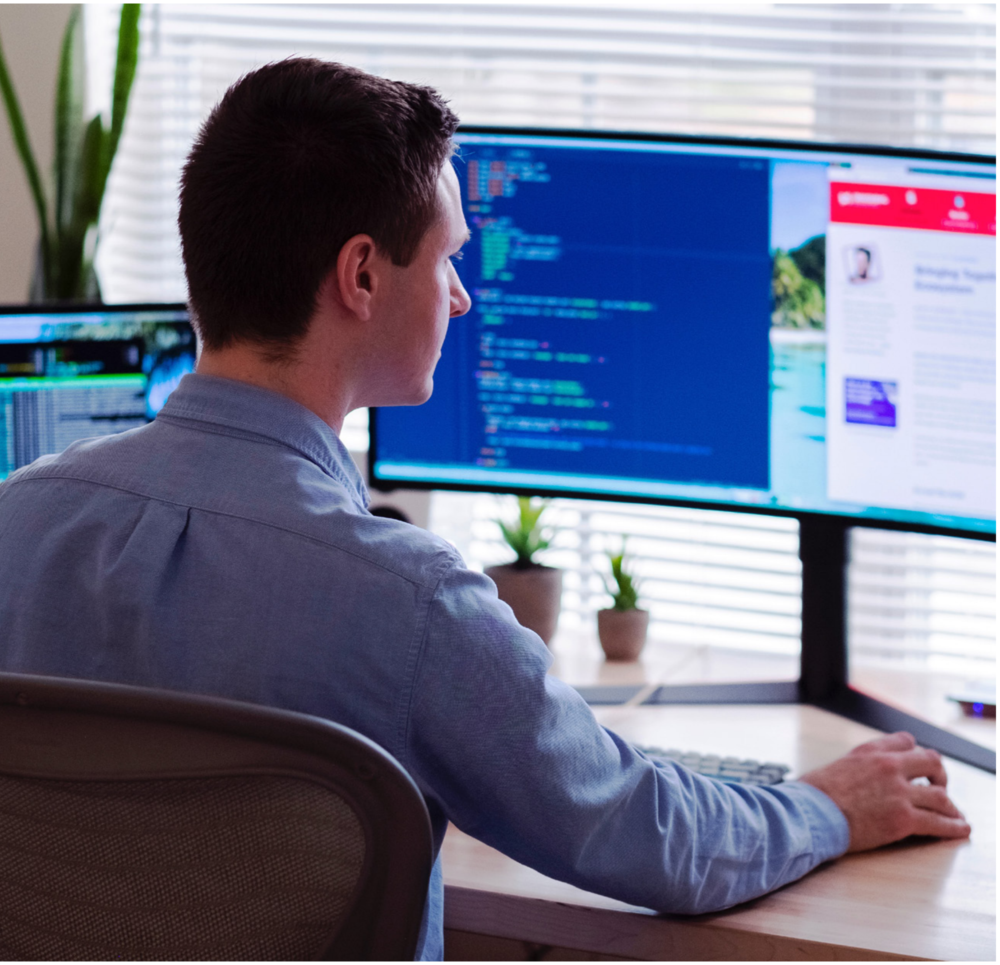
1. Data loss and security breaches.

a. **O365 is vulnerable** to internal threats (e.g., accidental deletion of data, actions by disgruntled employees, or access from ex-employees) as well as external threats (e.g., malware or ransomware).

b. **Malware attacks are a reality today,** and SaaS tools are no exception. Almost half (49%) of organizations have suffered from an unrecoverable data event in the past three years. And 69% of organizations have suffered successful malware attacks within 12 months, according to IDC research in 2018, 39% of which involved ransomware.

c. **An enterprise-grade backup strategy** can give enterprises an option to recover from security breaches by using granular recovery.

Risks without a backup plan.



2.

a. **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.

b. **Having a third-party backup can help** organizations set their own retention policies according to their business needs, as well as remain compliant with European data regulations.

Risks without a backup plan.

3 Lack of data control in hybrid deployments.

a. **Companies don’t always have full oversight of their data,** even though full oversight and control of data is a boardroom priority, and a first step toward becoming data-driven.

b. **Without backup, organizations do not have an exit strategy** or freedom from SaaS lock-in because they are not in complete control of their data.

Business-critical data.

Office 365 emails and documents – shared and stored in SharePoint, OneDrive, and Teams – are the new business-critical data.

From a business perspective, it’s difficult to deny the convenience of the SaaS model, especially when it comes to suites of applications such as Office 365, which add cloud-based collaboration capabilities to the task of creating and managing business-critical documents, email, and other content.

Business-critical data.

Office 365 offers integrated public cloud storage options in the form of SharePoint, OneDrive and Teams that can reduce the need for on-premises storage and simplify shared data access for collaboration.

There is a common misconception that SaaS-based customer data is secure and protected because it's already 'in the cloud.' In the case of Office 365, the licensing agreement clearly states that adequate data protection remains the responsibility of the customer.

This is where business IT has to step in and help key stakeholders determine the appropriate data protection, security, availability and retention policies for their data, and then match that to the right combination of technology. While this may add some complexity to SaaS adoption at the front end, a coherent, hybrid data protection plan will more than pay for itself in the event of a systems outage that can impact business-critical or compliance-governed data.

Business-critical data.

Today’s business environment increasingly depends on the documents, emails, and other business-critical information that is created, stored and shared within the Office 365 SaaS dataset.

This type of information is making up a growing majority of the on and off-premises data that’s being generated and stored as a critical part of modern business.

It’s easy to think that all data protection is alike, but there are major differences between protecting the Office 365 infrastructure and protecting customer data created and stored in Office 365. While the collaborative flexibility offered by shared SaaS storage is a positive, it only makes it more important for IT to help ensure that there is sufficient security to protect against a targeted intrusion.

Data backup.

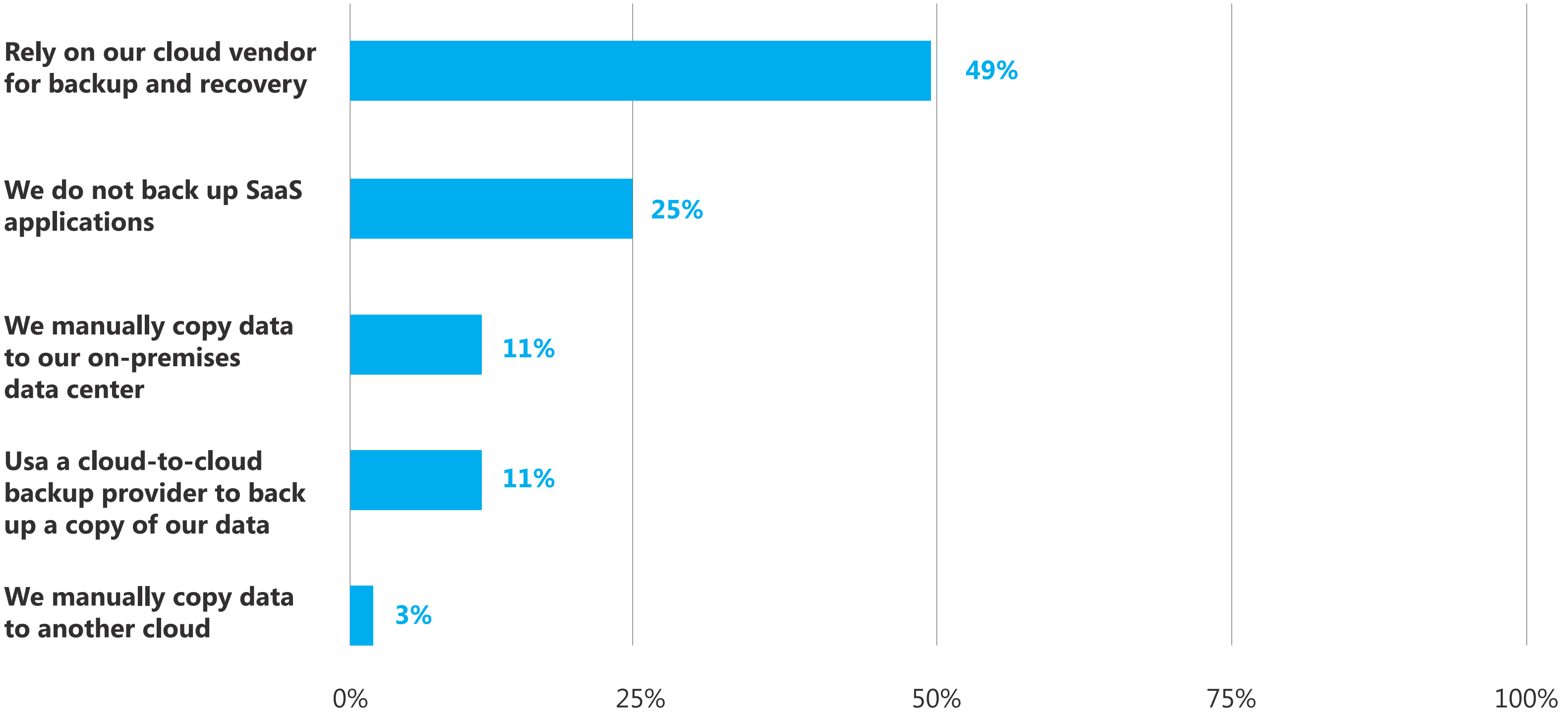
There is a common misconception that SaaS data in the cloud is inherently safe.

Data backup remains one of the key principles in data protection for several reasons, and while SaaS vendors focus on providing infrastructure resiliency and application availability for their own platform, the traditional 3-2-1 backup rule still applies as a best practice for ensuring data protection and resilience.

With SaaS data, the dynamics change because the original data may have been created and only exist on the SaaS vendor's cloud storage platform and should be backed up to a second, independent location – either to a separate IaaS cloud storage target or on-premises if dictated by industry-specific compliance requirements.

Data backup.

What is your organization’s primary data protection strategy for SaaS applications?



Percent of sample (n=427)

Data backup.

Only 11% of the respondents come close to addressing the primary need for a consistent and automated backup.

While it is not required that the backup be with a cloud-to-cloud backup provider, it is critical that it be independent of the cloud platform itself. Manual copying of any type can be inefficient and prone to errors, and the 25% that don’t make any backups at all are playing a dangerous and potentially costly game.

The highest percentage of responses trust their cloud vendor to do backup and recovery, but this is only a viable option if a SaaS vendor specifically offers full backup and recovery services. Most do not, and this misunderstanding can pose a major risk to business-critical data. It ultimately comes down to the best-practice rule that data should be backed up to a second system/location, be it cloud to cloud or cloud to on-premises.

Tier one cloud data centers are designed to provide top-level, 24/7/365 availability, security and resilience, but even with that remarkable degree of engineering, most cloud vendors themselves still recommend a model covering multiple data centers and/or availability zones to protect against outages.

The problem is that the replication-based model they use to protect their own systems is not the same as an independent backup of your SaaS data.

Data backup.

Expanded recovery and governance options are becoming nearly as important as the data backup itself.

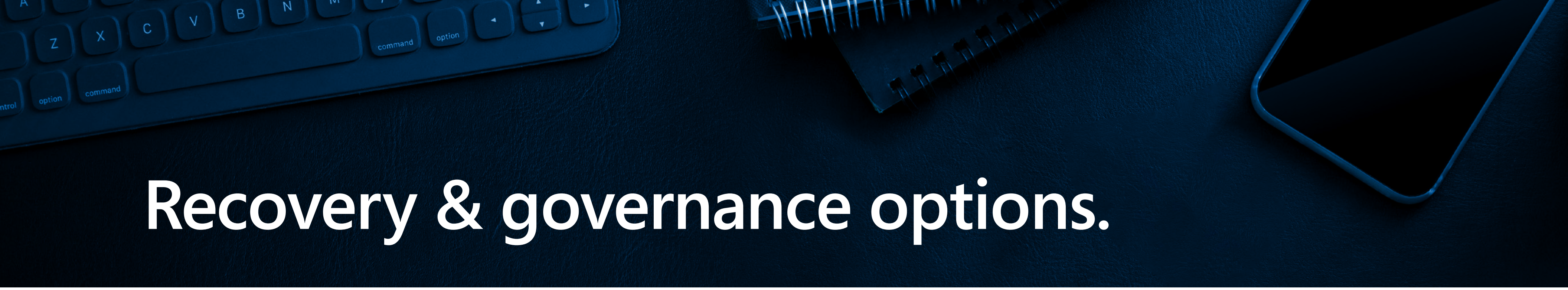
The newest risk for SaaS data comes from challenges created by privacy initiatives such as GDPR and the California Consumer Privacy Act of 2018, which is scheduled to take effect in 2020. GDPR became law in 2018 and applies to the processing of personal data from any business activity in the EU without regard to whether the processing occurs inside or outside the EU.

The regulation gives EU residents more control over their data. Individual powers include the ability to prohibit data processing beyond its specified purpose for collection, the right to be forgotten, and the ability to withdraw consent to the collection and use of personal data.

This can become a serious problem that is only made worse by the colossal amount of legacy data that's been piling up across the industry.

Appropriately protecting and managing all these emails, documents and sites can be a daunting task, but from a business perspective, it won't be long before the risks of not managing personal data could far exceed the cost of fixing the problem if found in violation.

The GDPR alone has penalties of up to €20m or 4% of a company's annual revenue, whichever is higher, for infraction. In the US, the proposed California Consumer Protection Act of 2018 adopts a somewhat different model based on a $7,500 fine for each violation. To put this in perspective, a CCPA violation affecting 500,000 accounts could potentially result in a fine of $3.75bn.



Recovery & governance options.

Another legal consideration that drives SaaS data protection is the e-discovery process that companies must undergo as part of a legal action.

When a company receives a subpoena for business data, that data suddenly becomes evidence, which changes everything. Depending on the scope of the request, it then becomes the company's responsibility to identify, preserve, collect and process that data to present to its legal defense team, who will then review and analyze that data for relevance and context, exclude privileged information and then prepare it for submission to the court.

A legal hold is a process for locking down data to ensure it's not deleted or modified in the process, and it's important to have the tools necessary to meet the granular protection and security needs of an e-discovery event. But a legal hold is something that needs to be used selectively, and though Office 365 offers broad legal hold capabilities, a full and independent backup copy of SaaS data may be the best approach for providing a point-in-time dataset for e-discovery purposes.

Unfortunately, the rules of evidence can vary substantially between jurisdictions, so a company should always refer to legal counsel before responding to a court order for digital evidence, and then follow that advice to the letter.

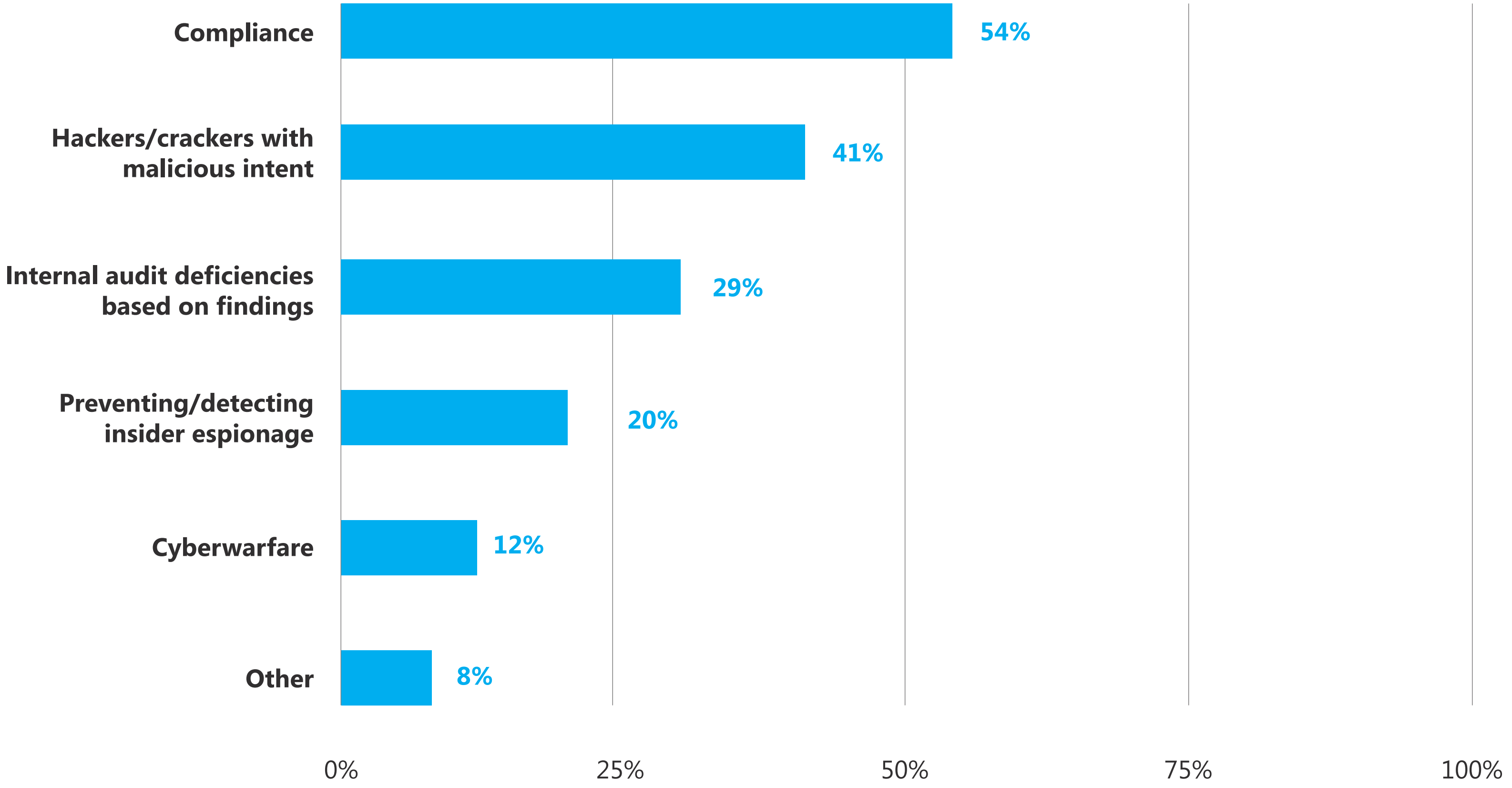
Legal compliance challenges.

Data protection will be increasingly driven by new legal and compliance-based challenges.

In 2018, a 451 VoTE security survey asked enterprise customers what their key security concerns were over the last 90 days, and it was telling to note that concerns about industry compliance exceeded those of threats with malicious intent.

Legal compliance challenges.

Top information security concerns within last 90 days



% of Respondents (n=99)

Legal compliance challenges.

Most of these security concerns align almost exactly to the most common vulnerabilities for Office 365 and other shared data environments.

These risks can be substantially reduced by a data protection schema based on the classic 3-2-1 rule for data backup and scheduled to meet appropriate RTO/RPO requirements.

Office 365 data that primarily resides in the cloud offers convenience and relatively high availability, but best practices still dictate that it should at least be backed up to a public cloud provider such as Azure or AWS, or alternately, on-premises to ensure greater accessibility and control.

Legal compliance challenges.

This points to the most important reason why you have a backup, which is data recovery.

An Office 365 backup offers data loss protection, but that can be of little value if data recovery is limited by factors such as bandwidth, connectivity, recovery granularity, failed backups, or the inability to recover to an alternative destination or format. IT administrators who focus on data protection – especially in the context of Office 365 data – are often tasked with a complex set of challenges when it comes to recovering specific data from a massive repository of backups, or the need to recover complete Office 365 datasets after a ransomware attack.

But administrator responsibilities can also be as mundane as recovering a specific email or file for a user, so having the right tools to do this as quickly and efficiently as possible frees up valuable time that could be used for more important business tasks. As a rule, any Office 365 backup strategy should have a matching recovery strategy that addresses data loss vulnerabilities both large and small, provides granular and directed recovery options, and includes a testing schema that evolves as changes are made in infrastructure, platform, or RTO/RPO requirements.

Conclusion.

a. **Know that Microsoft provides infrastructure resiliency and application availability within Office 365, but you are the data owner.** You are responsible for the protection of your own business data, and you should define data protection based on the specific needs of your business.

b. **Research and consider acquiring a third-party data backup solution.** It's one of the best ways to cover your business from data loss vulnerabilities related to Office 365.

c. **Plan to address threats** such as accidental deletion and internal and external security threats, and to meet mandated security or compliance requirements.

d. **Engage stakeholders in your business (and within your IT department) to set and test data recovery SLAs.** Test various data recovery scenarios within native SaaS platform tools and compare those with third-party backup products.

e. **Understand the specific compliance and legal rules of your business environment.** The laws surrounding data protection and security are always changing, and one of the key considerations of any data protection plan should be ensuring compliance.

ZONES
First Choice for IT™ | Microsoft | veeam

Zones and Veeam, developers of innovative products for virtual infrastructure management and data protection, can help customers reduce costs, minimize risks and fully realize the promise of virtualization. With our strategic partnership with Veeam, Zones has a proven track record of designing and implementing reliable backup and disaster recovery solutions that improve the speed of recovery and reduce costs.

Zones and Microsoft provide intelligent solutions to help you succeed in the future. As an authorized Microsoft Licensing Solutions Partner and a Tier 1 Microsoft Cloud Solution Provider, Zones offers the solutions, teams, and services that support an agile, engaged, and energized workplace.

First Choice for IT.™

Ready to see how Zones can help simplify O365 backups for you?

ZONES
First Choice for IT™

Visit **zones.com** or call **800.408.ZONES** today.

GET STARTED >