SPANNING
A Kaseya COMPANY

BEST PRACTICES FOR MICROSOFT 365 BUSINESS CONTINUITY

TABLE OF CONTENTS

INTRODUCTION

Whether it's due to human error, cyberattacks or natural disasters, unplanned downtime can happen at any moment, severely impacting your business, and in extreme cases, even shutting down operations permanently. The average cost of downtime can go up to $11,600 per minute, meaning long durations of unplanned downtime can hurt your business in more ways than one.[1]

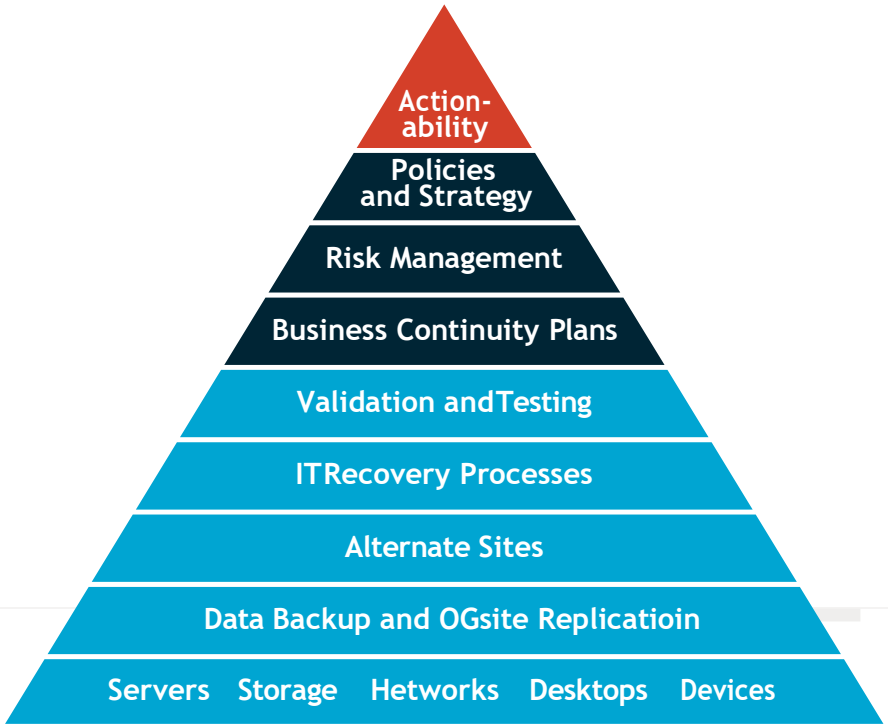
"BUT MY MICROSOFT 365 DATA IS PROTECTED BY MICROSOFT. WHY SHOULD I BE CONCERNED ABOUT DOWNTIME?"

While this is a valid question, you may not like the answer.

Here's the inconvenient truth: Although Microsoft provides a financially backed 99.9 percent uptime guarantee for Microsoft 365, customers are operationally and contractually liable for data protection. This raises a big question regarding business continuity – how does your organization continue to function when data loss incidents occur?

TRADITIONAL BUSINESS CONTINUITY FRAMEWORK

A typical business continuity framework is similar to a pyramid structure segregated into three sections. The bottom of the pyramid represents activities associated with disaster recovery, how IT professionals address each element and the amount of time and resources dedicated to each element. The middle section focuses on where the business must make strategic decisions and which IT element can then be incorporated into tactics. Finally, the top of the pyramid sheds light on enablement, communication and other activities needed to implement the plan. This is arguably the most important and neglected element.



Business continuity planning has traditionally focused on minimizing risks and mitigating the effects of large-scale, high-cost disaster events. Businesses develop business continuity or disaster recovery (BCDR) plans, and when something happens, they use the plan to manage responses, restore systems and data, take actions to mitigate the damage, review what happened and make changes to be better prepared for the next disaster.

While this model has served businesses well, in the case of Microsoft 365, the elimination of the infrastructure element has changed the nature of disasters IT professionals are likely to deal with. For instance, human error and malicious activity may not always result in large-scale, high-cost disaster events. However, they occur with much greater frequency, thereby increasing the chances of a major disaster occurring.

That said, organizations still need to develop strategies and tactics to minimize risks and mitigate the effects of large-scale, high-cost data loss disasters. At the same time, they also need to address common, smaller incidents that not only impact individual or team productivity but also extract a more subtle but significant cost.

While the fundamentals of traditional business continuity planning and disaster management are still relevant, in the SaaS world where Microsoft is wholly responsible for application availability, IT leaders need a new model of business continuity that is focused on security and data protection.

THE SHARED RESPONSIBILITY MODEL

Microsoft 365 follows the Shared Responsibility Model wherein the customer is considered the "Controller" of their data and the vendor acts as the "Processor" of that data. The terms controller and processor have been codified in regulations like GDPR, HIPAA and Microsoft agreement.

The agreement states that Microsoft is completely responsible for application availability and will provide a financially guaranteed SLA for 99.9 percent uptime. However, as a processor, it is their responsibility to add, delete or modify data upon request. And by request, we don't mean opening a ticket with Microsoft. We mean every user hitting the delete key on their keyboards or right-clicking on their mouse and hitting delete, or any process or script that deletes or modifies data.

That means if any malicious activity or accidental deletion request is authenticated by valid credentials, Microsoft will consider the request legitimate and honore it. As a result, accidental, malicious or fraudulent deletions, in all cases, are the responsibility of the customer/controller.

MICROSOFT EXPLICITLY OUTLINES CUSTOMER SECURITY RESPONSIBILITY:

THAT RESULT FROM YOUR UNAUTHORIZED ACTION OR LACK OF ACTION WHEN REQUIRED, OR FROM YOUR EMPLOYEES, AGENTS, CONTRACTORS, OR VENDORS, OR ANYONE GAINING ACCESS TO OUR NETWORK BY MEANS OF YOUR PASSWORDS OR EQUIPMENT, OR OTHERWISE RESULTING FROM YOUR FAILURE TO FOLLOW APPROPRIATE SECURITY PRACTICES THAT RESULT FROM YOUR FAILURE TO ADHERE TO ANY REQUIRED CONFIGURATIONS, USE SUPPORTED PLATFORMS, FOLLOW ANY POLICIES FOR ACCEPTABLE USE, OR YOUR USE OF THE SERVICE IN A MANNER INCONSISTENT WITH THE FEATURES AND FUNCTIONALITY OF THE SERVICE OR INCONSISTENT WITH OUR PUBLISHED GUIDANCE THAT RESULT FROM FAULTY INPUT, INSTRUCTIONS, OR ARGUMENTS.

MAJOR DISASTERS

Although Microsoft may have one of the best security infrastructures in place, a major disaster can still occur due to human error, illegitimate deletion, programmatic errors, malicious insiders, hackers, malware or ransomware.

SolarWinds was recently compromised as affiliated attacks leveraged Microsoft 365 instances and Azure applications hosted by Microsoft resellers. This allowed hackers to gain access and exploit the development environment of the SolarWinds Orion network monitoring platform.[2]

> "THERE ARE OVER 300 MILLION FRAUDULENT SIGN-IN ATTEMPTS TO OUR CLOUD SERVICES EVERY DAY. CYBERATTACKS AREN'T SLOWING DOWN, AND IT'S WORTH NOTING THAT MANY ATTACKS HAVE BEEN SUCCESSFUL WITHOUT THE USE OF ADVANCED TECHNOLOGY. ALL IT TAKES IS ONE COMPROMISED CREDENTIAL OR ONE LEGACY APPLICATION TO CAUSE A DATA BREACH."
>
> Melanie Maynes, Senior Product Marketing Manager, Microsoft Security

Sadly, the situation is getting worse. Phishing attacks have exploded since the COVID-19 outbreak. According to Symantec, around 135 million phishing attacks are attempted every day.[3]

Microsoft is frequently targeted by cybercriminals as threat actors sought to capitalize on vulnerabilities exposed by rookie remote employees working on networks devoid of company firewalls and other safety measures.

The real cost of a data breach

The IBM-Ponemon report stated that an average breach in the U.S. costs organizations $8.64 million and that businesses are 23 percent more likely to be breached now than ever before.[4]

However, the consequences of a data breach go beyond just financial loss. It causes business downtime and potential reputational damage, leading to loss of business and competitive advantage.

To get the right insights on the real cost of a data breach, you need to consider three types of costs that follow in the wake of a data breach: direct costs, indirect costs and non-compliance costs.

DIRECT COSTS

Following an attack, businesses go into investigative mode trying to determine the **what**, **how** and **why**. Businesses still using the trial-and-error approach often find that their investigation leads to three conclusions: close-to-accuracy, inaccurate or multiple reasonings with a high degree of variability. That's a lot of working hours to put into an investigation where conclusions are either full of errors or vague.

HERE'S THE DIRECT COST A BUSINESS INCURS RIGHT AFTER AN ATTACK:

TOTAL DIRECT COST = LOSS FROM ATTACK (LIKE RANSOMWARE OR HARDWARE MALFUNCTION)

+ WORKING HOURS INVESTIGATING ATTACKS + LOSS FROM POTENTIAL ATTACKS

INDIRECT COSTS

Ever wondered why publicized data breaches report losses in millions? Those figures comprise of direct and indirect costs – loss of business, disruption of business operations and lost productivity.

01

LOSS OF BUSINESS

Whether you are a small ad agency that has lost its latest creative work or a retail giant that lost an entire month's order, sudden data loss can cripple any business of any size. Mounting expenses coupled with a drying revenue stream pushes the situation to the extreme, leading to permanent business shutdown.

02

BUSINESS DISRUPTION

Recovering lost data can take hours, creating a logjam of ongoing work, which in turn creates a ripple effect, delaying work across departments.

03

LOST PRODUCTIVITY

In many ways, workplace productivity is the first casualty of data loss. The IT department needs to work overtime to recover lost data. Whether they succeed or not, you will still have to pay for overtime for a job that has no impact on your profit margins.

04

REPUTATION COST

Fixing the reputation of your business after a data loss is a tough nut to crack. In fact, reputation management can have a huge impact on your margins. Not only do you lose current customers but, with poor credibility and bad publicity, potential customers may never come knocking on your door again.

NON-COMPLIANCE COST

Compliance has always been a pre-requisite for regulated industries like healthcare and finance. However, with GDPR and CCPA, the need for compliance is extending to non-regulated industries as well. The surprising bit is organizations have been found non-compliant an average of six times by both internal and third-party auditors, resulting in an average of eight fines and costing an average of $460,000.[5]

PENALTIES

COMPLIANCE LEGISLATION	PENALTIES
HIPAA	Fines of up to $250k and 10 years imprisonment.
GDPR	Fines of up to €20 million or 4 percent of the total global turnover of the previous fiscal year, whichever is higher.
CCPA	Civil penalties of up to $7,500 for each violation. The maximum fine for other violations is $2,500 per violation.

LEGAL FEES

Fighting penalties means dealing with a pile of legal paperwork, courts and potential civil lawsuits as well. For instance, if a European citizen whose data was leaked decides to sue the organization in question, it could lead to a mountain of legal fees that can exceed the penalty itself.

RECERTIFICATION COST

A non-compliant business is expected to recertify employees in compliance training. This can be an overwhelming expense for clients that are already dealing with penalties and legal costs.

MINOR DISASTERS: EVERYDAY DATA LOSS

Major disasters tend to be the darlings of media outlets, often contributing to reputational loss for the affected businesses. However, everyday data loss, that has a bigger impact on business, is seldom discussed.

A recent IDC white paper, based on a survey of over 1,200 information workers and IT professionals, found that they spend an average of four and a half hours a week looking for documents. The IDC states that "They are spending half of those 4.5 hours searching for, and not finding, the files they need. Then they spend the other half recreating what they haven't found."[6]

The average cost of an office worker in the U.S. is $47,600 per year, which works out to $22.50 an hour, which means businesses are losing over $5,000 a year per worker's worth of productivity to lost emails and documents.

It isn't just productivity though. Lost emails and documents impact your revenue as well. Microsoft 365 is an integrated communication platform for businesses to connect with buyers and customers. High-transaction-value industries like real estate and finance usually have a complex sale cycle where comprehensive communication takes place over several months. If that email communication thread is lost, then needless to stay, it will impact current and potential revenue.

Considering the varying levels of importance of email communication to industry and business, it's almost impossible to come up with a solid average number to show the impact of lost emails and documents on revenue.

However, if data loss contributes to a loss of 10 percent of productive time, we can safely assume one percent of revenue is lost annually due to lost emails and documents. That's a dangerous number if you are a business that runs on tight margins since it could be the difference between being on the red or green side of the books.

1%

Lost Revenue Annually

4.5 Hours

Looking for documents every week

$22.50

Average hourly cost

$5,000+

Average annual cost per user

A NEW MODEL

WHY DO WE NEED A NEW MODEL FOR BUSINESS CONTINUITY?

Let's take a look at risk value, which is the standard metric for making BCDR-related investment decisions.

RISK VALUE = PROBABILITY OF EVENT x COST OF EVENT

Referring to IBM's data, the current risk value of a data breach is around $2 million. This is based on organizations with an average of 10,000 employees and $2 billion in annual revenue.[3]

Average organization size	10,000 employees
Average revenue per employee	$200,000
Average revenue per company in the survey	$2 billion

THE COST OF EVERYDAY DATA LOSS FOR THOSE SAME BUSINESSES COMES TO:

$50M
LOST PRODUCTIVITY

$20M
LOST REVENUE

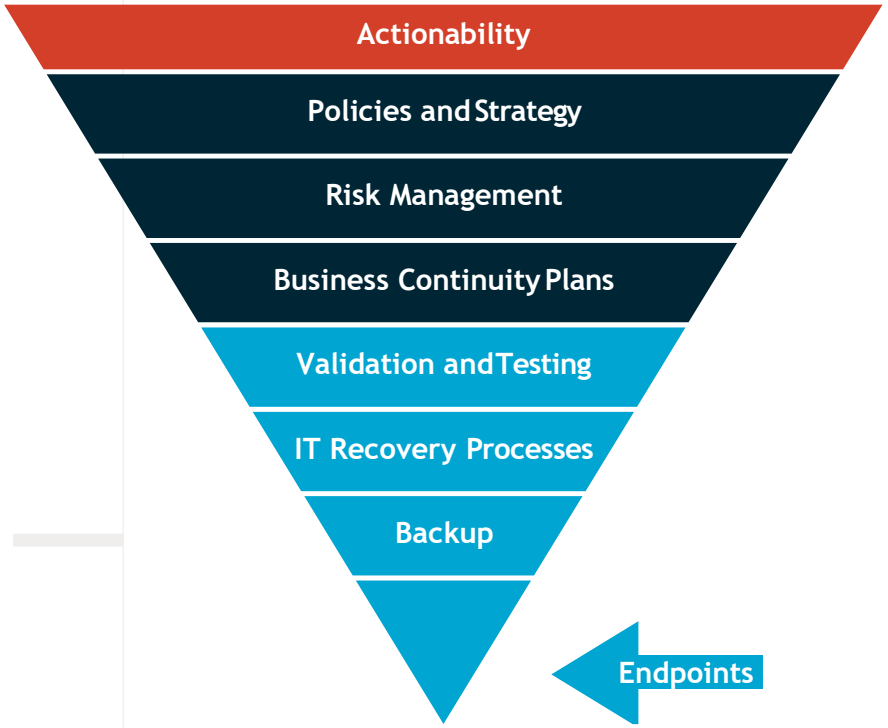
$70M
RISK VALUE OF EVERYDAY DATA LOSS

In fact, 77 percent of companies that use SaaS, report data loss events every year. And this just represents those large enough to be noted by IT.[7]

It's clear that the traditional disaster management cycle, which was designed to manage major disasters, failed to deal with the greater frequency and smaller scope of Microsoft 365 data loss events. That's why we need a more agile way to manage everyday Microsoft 365 data loss incidents.

We are going to take the traditional model of managing business continuity with a heavy focus on infrastructure and — turn it upside down. Add to that, we also learned with Microsoft 365 the concept of alternate sites is obsolete and so we will omit that. The new model will include disaster recovery elements that now focus primarily on data loss.

As a result, in the new SaaS model, businesses can invest more time and resources in developing business continuity plans that address a wider range of data loss events, and at the same time, focus on actionable activities enabling the entire organization – not just IT – to be more resilient.



MICROSOFT 365 BUSINESS CONTINUITY BEST PRACTICES

The new SaaS model empowers businesses to invest more time and resources on actionable activities.

A continuous incident management cycle helps manage the ongoing flow of data loss events and reduces both the frequency and severity of these incidents, with activities divided into three categories: prevention, anticipation, and mitigation.

Prevention

Strategies and tactics to minimize the risk of a data loss incident.

MFA IS A MUST, PERIOD.

Security experts across the board religiously recommend multifactor authentication (MFA) or two-factor authentication (2FA) to prevent unauthorized access to user accounts. It provides two layers of authentication – a password and an additional verifiable factor, like a one-time password (OTP) sent via SMS, or a biometric check like a scan of the fingerprint or retina. The best bit is its dual advantage. On one hand, it prevents Account Takeover (ATO) attacks and on the other, it keeps the user experience intact by not being too intrusive or demanding too much from users.

RESTRICT USER CONSENT TO AZURE-VERIFIED PUBLISHER

Allow user consent only for applications that have been published by a verified publisher. It's a simple, blue verification badge that appears on the application consent prompt. The blue tick signifies that Microsoft has vetted the application publisher and verified that they are a Microsoft partner and legitimate business entity. This protects you from consent phishing wherein sensitive data is accessed not by stealing your password but by tricking you into giving malicious apps the necessary permission to access your Microsoft 365 data.

THINK BEYOND MICROSOFT 365 EMAIL SECURITY

Microsoft 365 offers a built-in phishing and malware protection solution for incoming emails. However, because the solution is based on anti-spam technology, its native functionality is ineffective against more sophisticated, targeted attacks. Since 65 percent of ransomware infections are delivered via phishing, using an email phishing solution should be a top consideration.[8]

CONSIDER MICROSOFT 365 DATA LOSS PREVENTION

Data loss prevention tools use rules and policies to determine which files and data are considered confidential, critical or sensitive, and then protects those files from being shared or transmitted. The goal of applying these rules, policies and protective measures to Microsoft 365 is to prevent data loss from the Microsoft 365 environment.

CONTINUAL COMMUNICATION, EDUCATION AND TRAINING

Often, data protection tools and technologies are implemented with no communication of why they are needed or how to use them, leading to poor user adoption or Shadow IT. BC and DR plans are developed, documented and tested once by IT folks and then filed away forever. After all, out of sight is out of mind. The best defense against data loss is user enablement. A data loss prevention strategy is only truly effective when users are aware, educated and know exactly what to do in case of a data loss event.

Anticipation

Strategies and tactics to identify likely data loss incidents and related consequences.

LOOK OUT FOR THE UNUSUAL

There are tools for organizations of all sizes including native tools from Microsoft to monitor Microsoft 365 activity: examine potential security risks, track user behavior, understand how users create and share content, and more. Keep a keen eye on third-party SaaS applications that use Legacy Service Accounts. These accounts entail the risky practice of storing privileged credentials, generally without MFA. Essentially, one hack of your service account is all it takes for a data breach to occur, which can possibly go unnoticed for several months – seven months on average.[9]

USE SPARROW

If you are a major Microsoft 365 user, you should take advantage of a CISA's free tool Sparrow.ps1. It detects possible compromised accounts and applications in the Azure/m365 environment. The tool is intended for use by incident responders and focuses on the narrow scope of user and application activity endemic to identity and authentication based attacks seen recently in multiple sectors. It is neither comprehensive nor exhaustive of available data and is intended to narrow a larger set of available investigation modules and telemetry to those specific to recent attacks on federated identity sources and applications.

MANAGE ACCESS

Use Microsoft Cloud Access Security to improve access management, revoke access to those who no longer need it, or if their roles have changed. Once attackers are in the network, they will attempt to move laterally to access secure data. People who should not have access to sensitive data, but do, greatly increase the attack surface. If your organization uses more cloud applications than just Microsoft 365, you may want to invest in a third-party CASB to extend control to third-party apps and API connections.

IMPLEMENT A DARK WEB MONITORING SOLUTION

MFA is a must but it isn't perfect. Sophisticated hackers have developed methods to bypass second and third-layer security protections like MFA if users are not careful. For instance, Pioneer Kitten targeted Iranian dissidents by deploying malware in the victim's Telegram messaging app, whose MFA was bypassed using previously intercepted SMS codes.[10] Implement a dark web monitoring solution along with MFA to identify potentially compromised accounts before malicious action takes place.

Mitigation

Strategies and tactics to minimize the negative impact of data loss incidents.

PUT RUNBOOKS INTO ACTION

"Runbooks" document the procedures that should be taken when a data loss incident occurs. Organizations should create and publish user-friendly runbooks with procedures for departments, teams and individuals. While data loss incidents are an everyday occurrence for IT, hopefully your users aren't experiencing them often enough for them to be commonplace. Simple, easy-to-use runbooks with step-by-step instructions will provide you with more organizational resilience than just about any investment in technology.

USE AN MICROSOFT 365 BACKUP SOLUTION

The harsh truth is Microsoft 365 data loss is virtually inevitable. You need an Microsoft 365 backup with fast and easy, granular, point-in-time data restoration functionality – recover your precious business data stored in Exchange Online, SharePoint Online, OneDrive and Teams.