RESTECH SOLUTIONS

WHAT'S LURKING IN YOUR SERVER CLOSET?

CYBER MONSTERS AND DATA LOSS

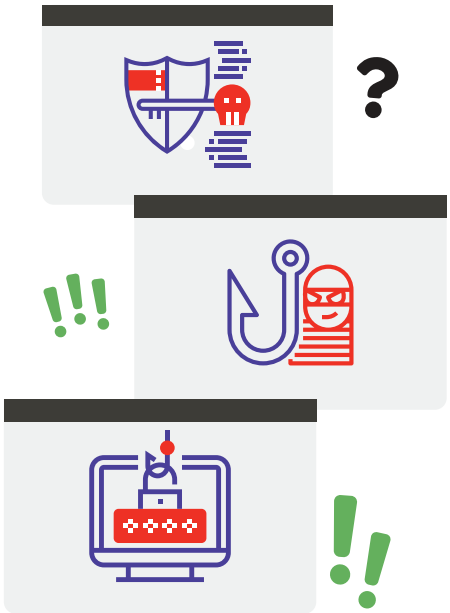
Your minds start to wander as you glance over your backup logs, hoping that today isn't the day the monsters come out to play.

Welcome to the life of small and medium-sized businesses (SMBs). On the surface calm, cool and collected – masters of their domain. Yet, deep down, they know something is lurking in their server closets and beyond — monsters that cause data loss, downtime and bleed businesses dry.

Businesses everywhere are constantly looking over their shoulders thinking, ***"what if I'm next?"***

Unfortunately, it isn't a matter of if but when.

This eBook aims to shed light on the cyber monsters that cause data loss, wreak havoc in your production environment, delay strategic initiatives and trigger major business losses. This eBook also provides solutions on how to bring an end to their reign of terror, allowing businesses to concentrate on their growth without worry.



RESTECH SOLUTIONS

LIMITATIONS OF SOFTWARE-AS-A-SERVICE (SaaS)

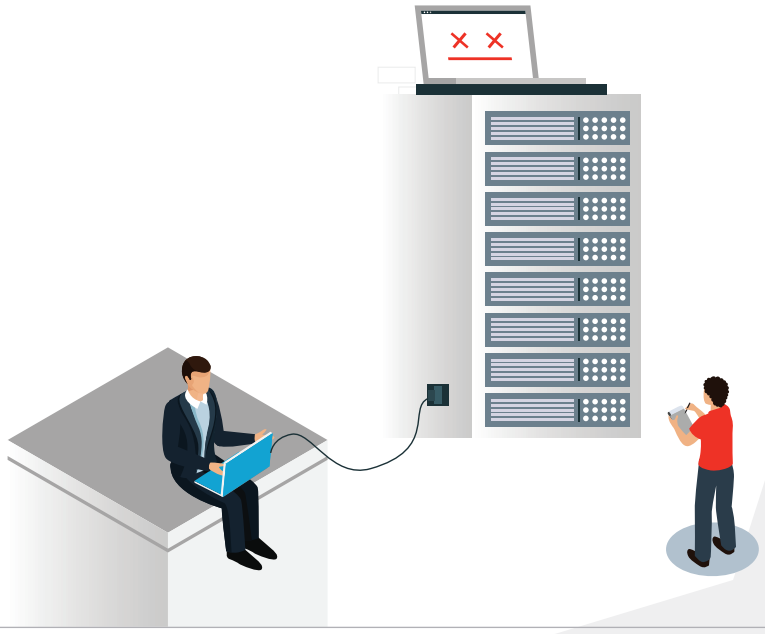
Many are still clueless about the limitations of native data protection capabilities among SaaS providers.

The usage of SaaS applications like Microsoft 365 and Google Workspace has exploded in recent years thanks to rapid digital transformation. However, despite this rise in popularity, there are still misconceptions about who is responsible for data protection.

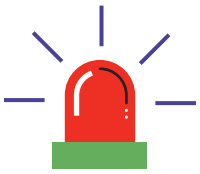
SaaS providers like Microsoft 365 follow the Shared Responsibility Model, where the customer is considered the "controller" of the data and the provider acts as the "processor" of that data. As a processor, it is their responsibility to add, delete or modify data upon request. That means if any malicious activity or accidental deletion request is authenticated by valid credentials, the processor will consider the request legitimate. As a result, accidental, malicious or fraudulent deletions, in all cases, are the responsibility of the customer/controller.

Sadly, many IT pros and businesses are either unaware or ignore the obligations that come with the shared responsibility model, and operate under false assumptions. For instance, SaaS applications have native solutions to protect data. In reality, these built-in features are usually archival solutions. That means deleted data is stored for a limited period only and restoring it can be a slow, cumbersome nightmare.

The bottom line is operational and contractual responsibility for SaaS data lies firmly in the hands of the users and not the SaaS vendors. Ignoring this fact can severely damage your business.



RESTECH SOLUTIONS



OVERLOOKED COMPLIANCE MATTERS

Fear of compliance matters and negligence prevents businesses from keeping a disaster recovery (DR) plan on par with required standards.

Granted, DR testing can be challenging — right from keeping up with environmental and personnel changes to having the required time and resources to properly test. However, not testing leaves businesses in the dark regarding the effectiveness of their DR plans. In effect, they are left with a "living dead" DR.

A well-crafted DR plan increases the possibility of a business recovering lost data and resuming normal operations with minimal disruptions. It's a missed opportunity, not to mention a huge risk, to put in the hours and resources to create a disaster recovery plan only to then not test it. One of IT-based businesses' greatest nightmares is realizing that their non-tested DR plan isn't working as intended, and by the time this realization hits, they're already in the middle of a disaster – which is exactly when the DR plan is supposed to work.

In sectors like healthcare, finance and government, strict compliance standards like HIPAA and FINRA demand a disaster recovery plan with a specified uptime. Accurate assessment of uptime and gauging whether defined recovery time objectives (RTOs) can be met is not possible without DR testing.

A lack of DR testing leads to long hours of unplanned downtime that can cost businesses huge amounts of money depending on the size of the business, not to mention penalties and legal fees that arise from non-compliance. With these kinds of losses, businesses might very well join the ranks of the walking dead.

RESTECH SOLUTIONS

HERE ARE THE PENALTIES AND LEGAL FINES FOR NON-COMPLIANCE.*

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

PURGE ALL CLOSET MONSTERS WITH UNIFIED BCDR

Unified BCDR is your one-stop solution for slaying cyber closet monsters that take away the peace of mind of businesses. Protect data across physical data centers and virtual and SaaS applications with ransomware detection, self-healing backups, dark web monitoring and much more.

RESTECH SOLUTIONS

EASY SaaS DATA PROTECTION

A unified BCDR solution provides powerful, yet easy-to-use SaaS data protection for Microsoft 365, Google Workspace and Salesforce. It allows administrators and users to restore data and get back to work in just a few clicks, and it's backed by enterprise security and compliance.

NO DR SURPRISES

A unified BCDR solution with Recovery Assurance performs the highest level of application recovery testing with no IT time or effort. It fully restores applications, performs analytics, measures recovery time and recovery point, and identifies reasons why recoveries failed.

Detecting cyber monsters capable of causing data loss is far from simple and can drain a lot of your time and effort. As a result, it's always best to work with an expert, such as ourselves, who can help you through the process. Please do not hesitate to contact us if you would like to schedule an appointment.

RESTECH SOLUTIONS

Source:
Ebook-roi-microsoft-office-365-backup.pdf

713-936-6855
info@restech.solutions
https://restech.solutions/contact