eBOOK

Backup and Disaster Recovery in a GDPR World

INTRODUCTION

The General Data Protection Regulation (GDPR) is designed to further the protections around the privacy and integrity of personal data of EU citizens. One of the key changes implemented by the law enhances the rights of the data subjects, which includes a data subject having access to their personal data, requesting that it be ported, and restricting the processing of such data. The MSP armed with a proper managed backup and recovery solution is better prepared to meet the challenge of honouring these data subject requests.

Fortunately, most MSPs already prioritise daily and incremental backups and have a fair understanding about how to execute a business continuity plan. Even if there weren't compliance or security concerns to consider, having your standard services contract include robust hybrid cloud backup simply makes a lot of sense.

The MSP armed with a proper managed backup and recovery solution is better prepared to meet the challenge of honouring data subject requests.

A WORD OF CAUTION

MSPs looking to offer backup as part of a security-as-a-service or compliance-as-a-service offering need to choose their backup product wisely to make sure the fundamental GDPR data protections are in place.

For example, the product must offer strong encryption for backups. There is no excuse for having an unencrypted backup. This also includes any removable media being used as a speed vault or local backup repository. To ensure backup integrity, the software must include a robust encryption algorithm to protect all of your data. Additionally, all data should be encrypted in transit to the hosted storage facility and remain encrypted when in storage.

If you lose an unencrypted backup due to a cyberattack, misconfiguration, or physical theft, you may have to report this to the proper authorities and/or face potentially severe GDPR fines. So make sure your backup solution provides proper encryption.

TESTING YOUR BACKUPS

As a successful MSP, you probably already perform daily backups and even an occasional recovery check. But if you have a great backup solution, you can also automate a “test” recovery to ensure your backups will work when the time comes to use them. It could be embarrassing for your business and potentially damaging for your customer if you find out during a disaster that a backup doesn’t work. But if you regularly check the backup report and test recovery report, you’ll be more confident during a crisis (and show your clients that you’ve responsibly handled their backup even if the restore fails). Additionally, these reports could be useful to show GDPR authorities a good-faith effort on your part.

If you have a great backup solution, you can automate a “test” recovery to ensure your backups will work when the time comes to use them.

MSPs struggle when a security incident requires recovery of multiple systems or when workstations have complicated or unusual configurations. This makes a powerful point for cloud services. If your customers receive business services via web applications from third-party providers, they’ll have less to worry about in an availability security incident.

TIPS FOR RECOVERY PLANS

Here are a few points to consider when building a disaster recovery business continuity plan (DR/BCP) service offering for customers.

1. *Set expectations with the customer before an incident.*

   It's vital to establish a plan and set the costs for extraordinary and catastrophic circumstances. Having this conversation in advance can considerably reduce anxiety on both sides during an incident. For example, if recovery depends on specialized equipment, multiple unique configurations, or software license keys, it might take you longer to recover than your customer would expect. It's important to be upfront on what you, as an MSP, can deliver.

2. *If your workstations have been customized by users, then you should back up both workstations and servers.*

   In small and medium enterprises (SMEs), many applications can be dependent on specific endpoint configurations. Also, laptops often contain a significant amount of important data copied on their local drives. A good DR/BCP considers the importance of the endpoint user profile data—while it may be a pain restoring something as trivial as a user's shortcuts, you'll be glad you had endpoint protection in the event you have to recover a customer CFO's year-end spreadsheet. Although many MSPs insist information must be on the server for backup, you'll have happier customers if you also back up important data on endpoints.

3. *Try to virtualise servers and deliver business services from third-party hosting.*

One of the largest challenges found in SME environments is legacy hardware. It's not uncommon for SMEs to use servers that are five years old (or even older). If this is the case, older hard drives, proprietary interface cards, or even compatible power supplies may be difficult or impossible to find quickly in a disaster—especially if the server is nearing its end-of-life or is no longer under warranty. If the business or the MSP lacks spare hardware to assist, recovery could be delayed.

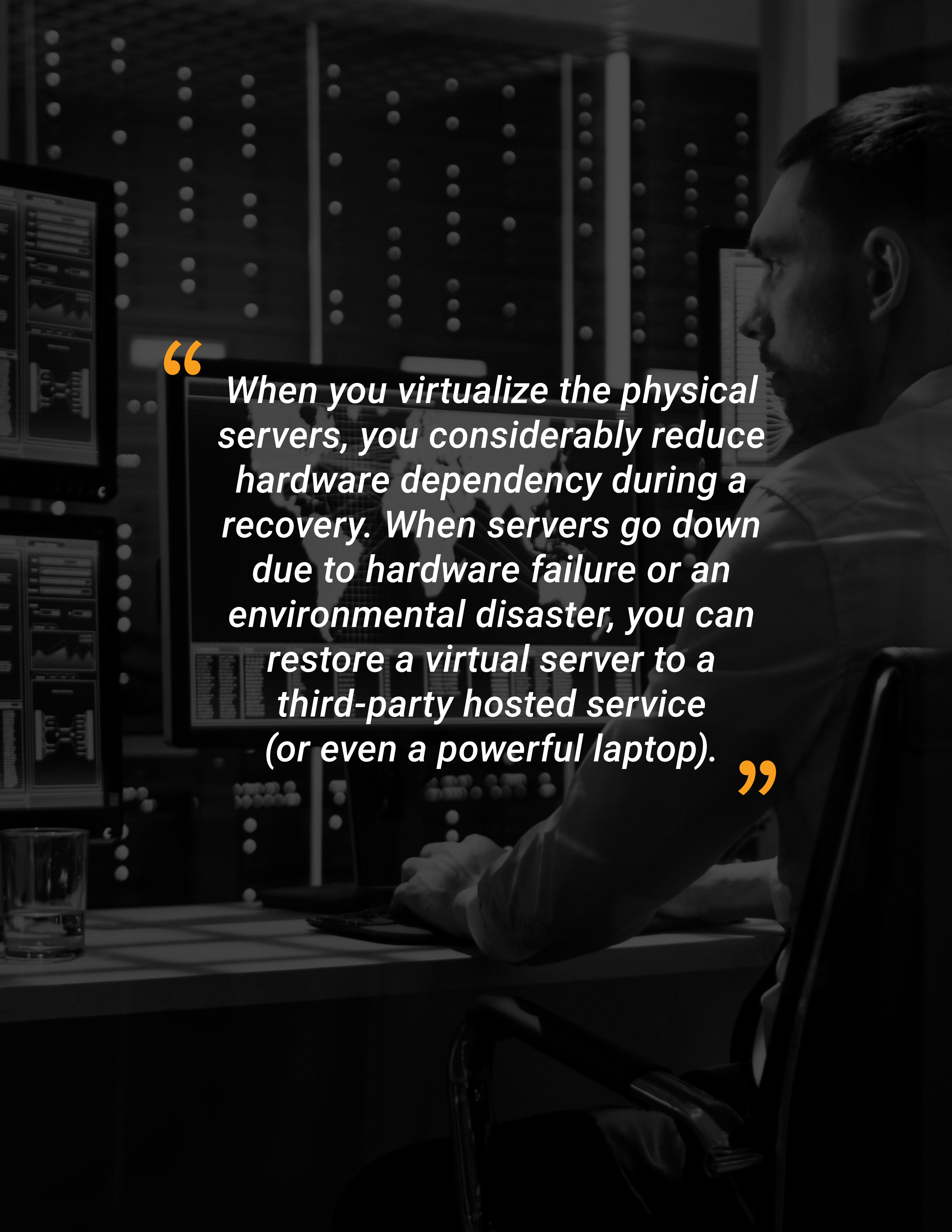
Enter virtualisation. When you virtualise the physical servers, you considerably reduce hardware dependency during a recovery. When servers go down due to hardware failure or an environmental disaster, you can restore a virtual server to a third-party hosted service (or, frankly, even a powerful laptop).

Even better, you should encourage your customers to move critical services to either third-party hosting or software-as-a-service providers. If email communications or customer relationship management (CRM) systems are the most important business services, moving them outside the business's physical environment may speed recovery considerably (if recovery is even required).

4. *Solid state drives (SSD) can be a huge win when used as a storage vault or backup data repository.*

If your BU/DR strategy includes hourly "snapshots" of databases and/or files, SSDs provide an excellent recovery option in the case of ransomware. The SSDs' incredible read/write speeds efficiently provide phenomenal backup throughput for the local copy. This local copy can then be transferred to the hosted facility outside of business hours to reduce bandwidth bottlenecks during productive times.

Systems with high disk activity (such as database servers, mail servers, or Microsoft® Exchange™ or SharePoint® servers) usually work hard and tax resources during business hours. Offloading backup snapshots to an SSD drive via iSCSI or USB-3 interface helps to reduce the potential of backup activity impacting the responsiveness of the servers.



> “When you virtualize the physical servers, you considerably reduce hardware dependency during a recovery. When servers go down due to hardware failure or an environmental disaster, you can restore a virtual server to a third-party hosted service (or even a powerful laptop).”

USING BACKUP FOR UPGRADES

The right backup product can also make server upgrades and migration products go much smoother. MSPs should take full advantage of backup products that allow them to take full system images and turn them into a bootable virtual server. It's easy to upgrade a server using virtual images created by a backup product and then deployed to the new host. In fact, the backup and recovery capability can facilitate a project to move servers off legacy hardware to a hypervisor or VMware® ESXi host.

In extreme circumstances, the image can run from a cloud-hosting facility or from a portable hard drive attached to a high-quality laptop (gaming laptops can be helpful here, believe it or not). You can easily find USB-3 drives in SSD format with 250GB or 500GB, and you can download VMware player for free (although, you need to buy a license for commercial purposes). With these two tools, you can provide instant BCP/DR using a super charged laptop with lots of RAM and a few portable SSD drives.

GDPR includes a number of data subject rights, including the right to erasure, also known as the right to be forgotten, which allows individuals to request that their personal data be erased. This obviously presents some complications for providing backup services.

Make sure to consult with your customers to plan for such requests. Please be aware that GDPR does have provisions for data retention for lawful processing and other legitimate interests, including non-EU laws and statutes, which may have data retention requirements for "business records." As always, we highly recommend you speak with a legal expert on the matter before finalizing your plan.

MSPs should take full advantage of backup products that allow them to take full system images and turn them into a bootable virtual server.

GDPR REQUIREMENTS ON DATA COLLECTION AND STORAGE

Under GDPR, one of the means to legally process personal data is explicit consent from individuals before a business can collect or process data. This means businesses, whether MSPs or their clients, must disclose what information is collected, why it is being collected, and how long it may be retained.

For example, some laws require that invoices from accounting systems be retained for seven years or longer. Court and health care records can in some cases have a lifetime or indefinite retention period. Alternatively, marketing data on an email list can often be erased per direction from the individual. The key is to set retention periods per the advice of legal counsel, a privacy consultant, or in the best-case scenario, a Data Protection Officer (DPO) under the GDPR.

The MSP providing backup needs to work with the business to facilitate requests by EU citizens. It could save time and make things far more efficient if you work with legal counsel or a DPO ahead of time to write template responses to common requests. For example, consider planning ahead to have responses ready to go for erasure requests, access requests, and any other potential GDPR requests. In the event of erasure requests, for example, it's worth asking legal counsel to help you explain any data that you cannot remove due to other legal retention periods.

GDPR AND BACKUP

GDPR introduces challenges for any MSP that provides backup services. Depending on the nature and complexity of the type of personal data being collected, stored, processed, or transmitted, backup plans must balance legal retention requirements while remaining flexible enough to accommodate the rights of EU citizens under the new law. It appears the days of backing everything up and storing it indefinitely could be coming to a close.

As an MSP providing backup services, you will have to manage your customers' expectations, plan for availability security incidents, and architect critical services for both redundancy and resiliency.

This document is provided for informational purposes only and should not be relied upon as legal advice or to determine how EU General Data Protection Regulation (GDPR) may apply to you and your organization. We encourage you to work with a legally qualified professional to discuss GDPR, how it applies specifically to your organization, and how best to ensure compliance. SolarWinds MSP makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including the accuracy, completeness, or usefulness of any information.