

VMware Data Protection Report 2010

The Survey of 500 Enterprises

ANNUAL REPORT

November 2010

Contents

Executive Summary	3
Survey Background	4
Introduction: Virtualization in the Enterprise.....	4
Mission-Critical Platform.....	5
Approaches to Virtualization Backup and Recovery.....	7
Management Concerns.....	7
Wrong Tool for the Job.....	8
Virtual Mindset.....	10
Backup and Recovery Assurance.....	11
Overcoming the Physical Mindset.....	13
Testing Backups.....	14
Recovery Times.....	17
Thinking Beyond the Impossible.....	18
Summary and Conclusions.....	18
About Veeam Software.....	19
vPower.....	19
Accelerating the Use of Virtualization.....	19

Executive Summary

The significant cost, power and efficiency advantages of server virtualization are accelerating its adoption across the enterprise, and this trend holds the potential for all IT infrastructures to become virtual estates, including those that move to an “IT as a service” model based on private and public clouds. With the penetration rate of virtualization in the enterprise approaching 50 percent, CIOs must now look beyond the “low hanging fruit” of virtualizing file, print, and web servers and departmental applications towards mission-critical applications such as email, CRM, ERP, and databases.

However, IT departments are now finding that virtualization is presenting entirely new risks and management challenges. The following report outlines key findings from a worldwide study on virtualization and data protection. It includes trends in the current state of virtualization adoption in the enterprise, and a review of current approaches to virtual machine backup and recovery. It highlights how enterprise adoption of virtualization is actually being hampered due to fears around the ability to successfully back up and recover virtual machines. For example, nearly half of businesses are not virtualizing mission-critical workloads due to concerns around their ability to backup and recover virtual machines.

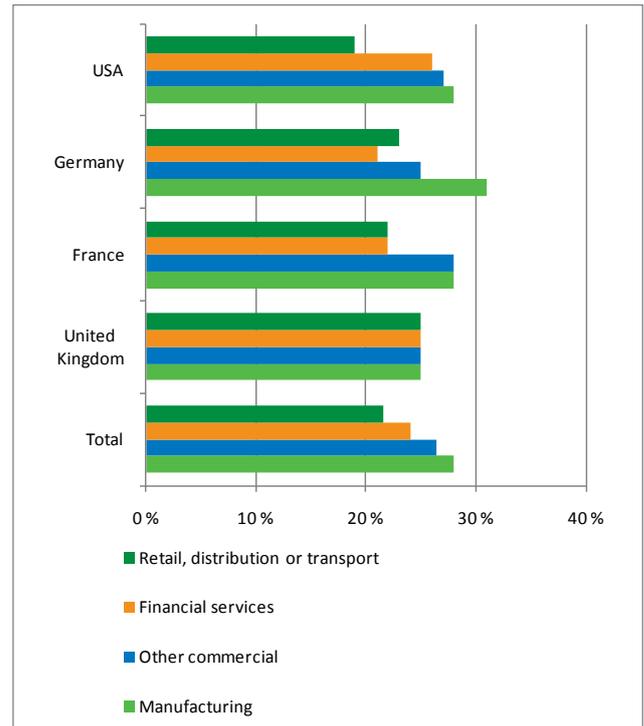
The findings highlight how virtualization should move from being viewed as a risk to an enabler of improved data protection within the enterprise. Enterprises must consider changing or augmenting their current management and data protection processes to take full advantage of virtualization technology.

The concluding section calls for a transformation of enterprise-level data protection strategies. More specifically, it outlines the need for an entirely new category of solutions based on virtualization that enable advanced data protection capabilities that are either very expensive or not possible at all with traditional data protection and disaster recovery tools.

Vanson Bourne, an independent market research organization, conducted an online survey in August 2010 of 500 CIOs from organizations across the United States, United Kingdom, Germany, and France that employ more than 1,000 people.

Survey Background

The organizations in the research survey had a wide geographical spread of employees, with over half of the businesses in the sample having employees based overseas. In addition, the companies were diverse, with the sample split almost equally between manufacturing (28 percent); financial services (24 percent); retail, distribution & transport (22 percent); and other commercial (26 percent). This ensured that the statistics generated were gathered from many different types of commercial organizations across different market sectors.



Types of organizations responding to the survey

Introduction: Virtualization in the Enterprise

In order to fully understand the implications of virtualization for data protection, it is first important to understand the true pervasiveness of this technology within today's typical enterprise-level organization. Here the research revealed some interesting trends, most of which may come as no surprise but at the same time highlight how critical it is to ensure that data protection strategies are capable of keeping pace with implementation of this technology.

Physical server consolidation remains by far the top benefit of virtualization for many enterprises (71 percent). Nonetheless, after consolidation, improved disaster recovery (54 percent) and data protection (51 percent) are the top two most important advantages of adopting this technology globally and in many regions.

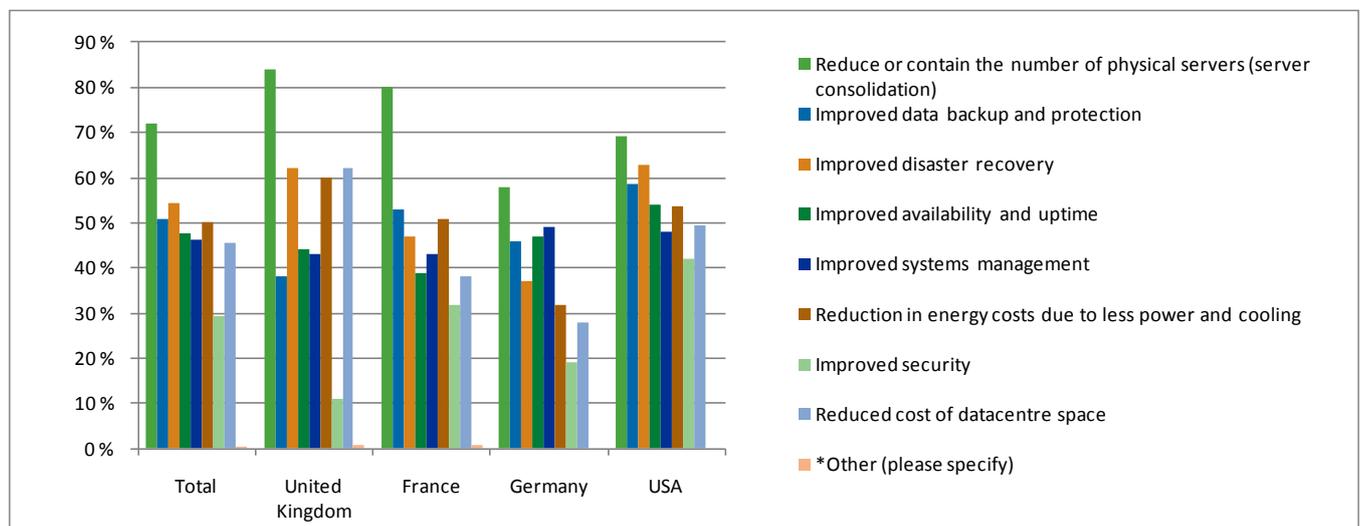


Chart 1.1: Key benefits of virtualization

Not surprisingly, Microsoft Windows (86%) is by far the most frequently virtualized operating system. According to the research, around 45% of businesses are using virtualized Linux-based servers.

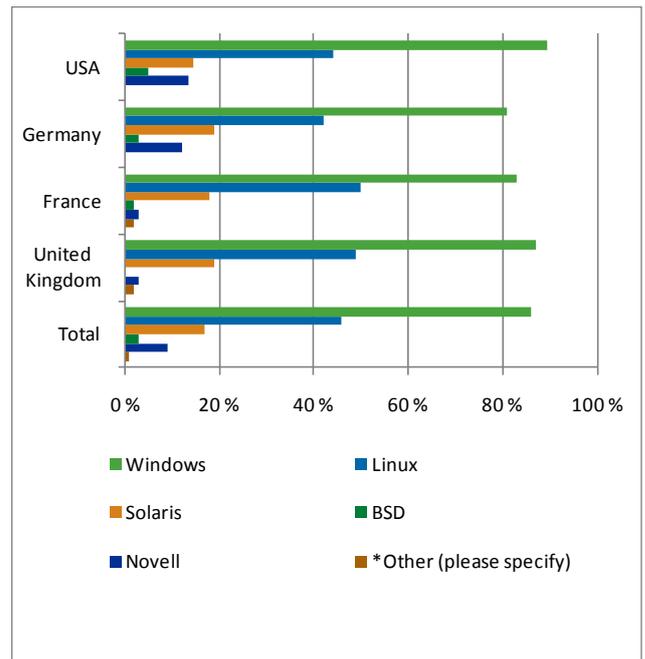


Chart 1.2: Operating systems currently used on virtual machines

Mission-Critical Platform

The unprecedented adoption of virtualization continues to grow, reaching the most important part of the IT estate - mission-critical enterprise applications. Enterprises are virtualizing an average of 42 percent of their datacenter/server estates today and expect that this will grow to 63 percent in the next two years. In fact, the popularity of virtualization is in essence establishing this disruptive technology as the de facto platform within IT environments. This trend is only set to continue.

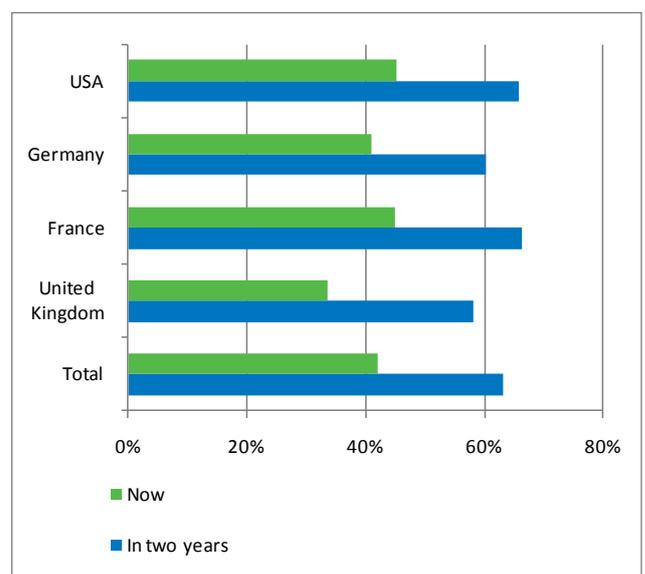


Chart 1.3: Percentage of datacenter/server estate virtualized now and in 24 months

Based on the findings above, on average, approximately half of all servers are viewed by CIOs today as mission-critical, and with 42% penetration, virtualization is fast approaching mission-critical applications.

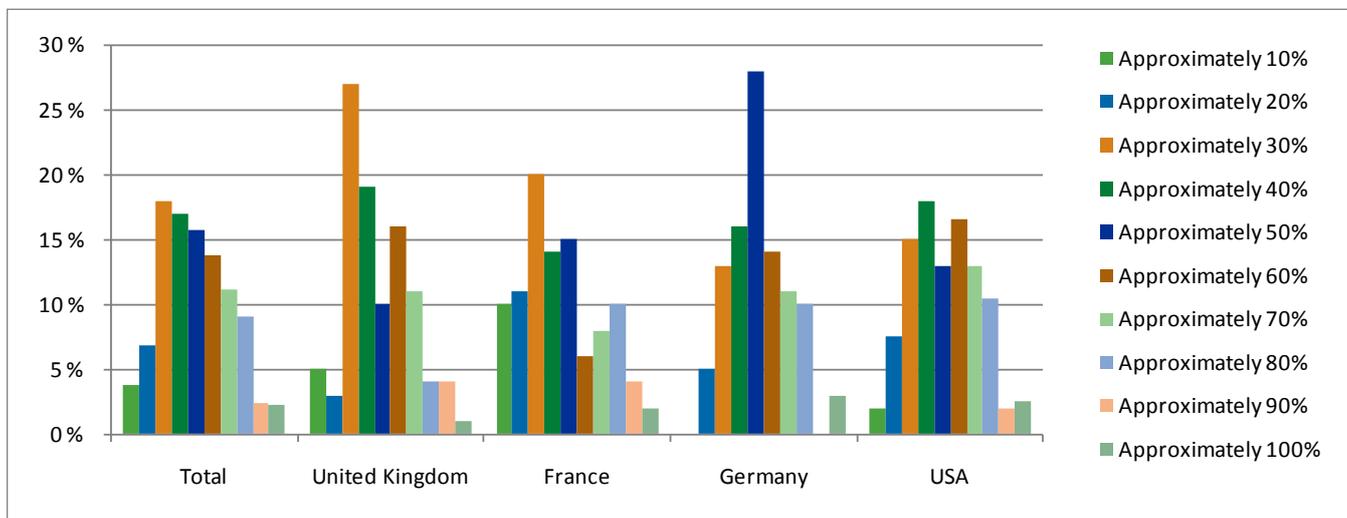


Chart 1.4: Percentage of servers viewed as mission-critical

Businesses are using virtualization for a broad range of workloads from web servers to ERP/CRM applications. It's therefore not surprising to see that in line with increased use of this technology, more and more business-critical workloads will be virtualized by mid-2012.

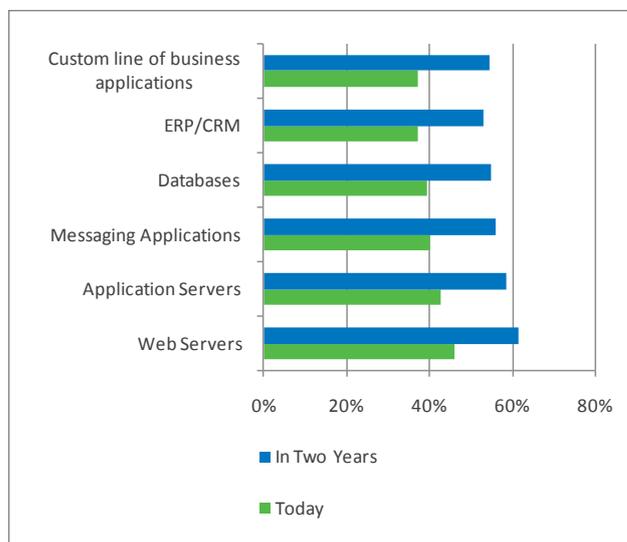


Chart 1.5: Percentage of applications on virtual servers today and in the next two years

Alongside the increased investment, over the long-term it is also likely that enterprises will seek greater choices around virtualization solutions. Indeed, although VMware vSphere is the clear market leader today (73 percent), the research highlighted how businesses are now looking to increase adoption of the Microsoft Hyper-V and Citrix Xen platforms from 28 percent and 27 percent respectively to 30 percent over the next 12 months.

While much of this data is likely to be corroborated by other vendors and experts in the field, in our view what's missing is a clearer picture of the management implications for virtualization. In order to explore this in more detail, it is first important to build an understanding of exactly how virtual machines are being managed today. More specifically, our research focused on current approaches in the backup and recovery space.

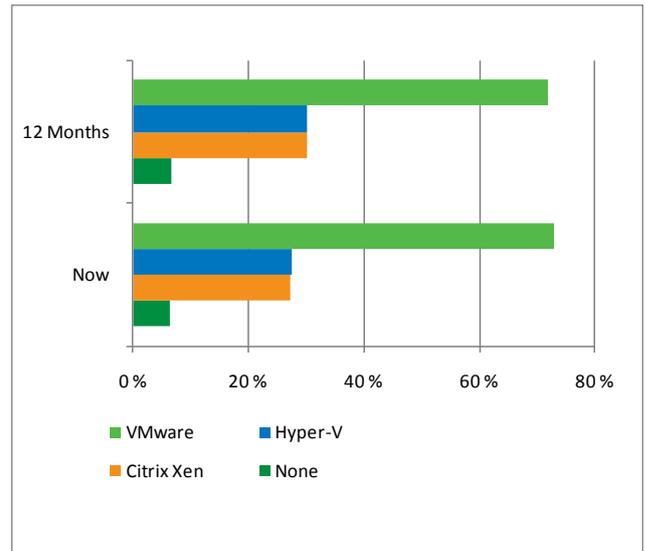


Chart 1.6: Use of VMware vSphere, Microsoft Hyper-V or Citrix Xen now and within the next 12 months

Approaches to Virtualization Backup and Recovery

Management Concerns

Despite the growing trend of businesses transitioning more and more of their applications to virtual servers, particularly for mission-critical workloads, the research highlighted some areas of concern. Specifically, enterprise adoption of virtualization is actually being hampered due to fears around the ability to successfully back up and recover virtual machines. Nearly half (44 percent) of respondents indicated that concerns around backup and recovery prevented them from virtualizing certain mission-critical workloads.

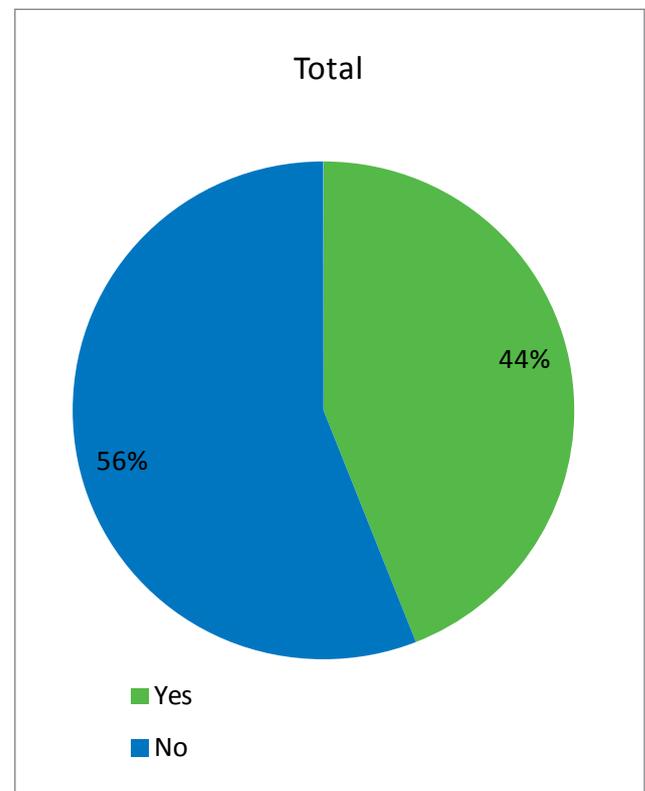


Chart 2.1: Percentage of enterprises not virtualizing mission-critical workloads due to concerns around backup and recovery

On average, only 68 percent of production-level virtual estates are currently being backed up; more specifically only 29 percent of organizations back up their entire virtual estates. This may not be an immediate cause for concern, as even in the physical IT environment not all data is backed up. Naturally, the research highlighted how businesses applied stronger processes to backing up critical servers over

non-critical (both virtual and physical). However, given the cost and resource efficiency of virtual machines in areas such as hardware and storage, it is reasonable to question why enterprises are still making choices around what is backed up and what isn't - one could argue that in an ideal world, it's important to protect all data, whether it's mission-critical or not.

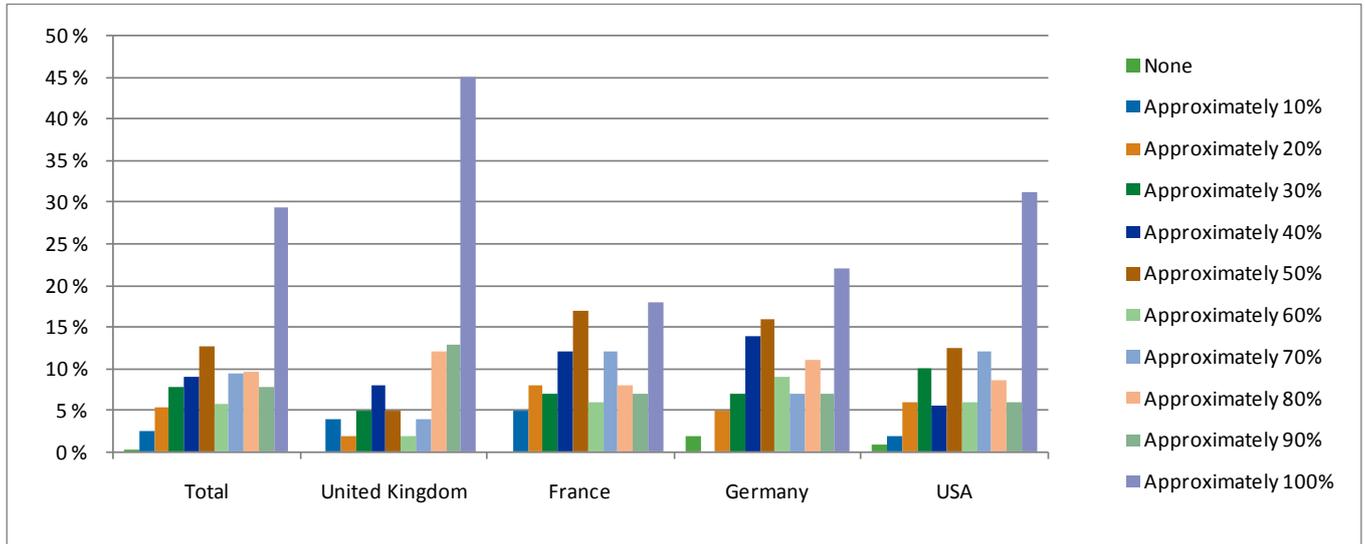


Chart 2.2: Percentage of production-level virtual servers being backed up

Wrong Tool for the Job

Part of the virtual machine backup issue can be associated with current approaches to backup and recovery. Virtualization is clearly a fundamentally different platform than physical infrastructure, yet nearly two-thirds (63 percent) of enterprises today use a single product to back up both physical and virtual estates. With this approach they are still treating virtual machines as physical servers and thereby limiting their ability to use the technology to its full potential. Consequently, enterprises do not have the optimum level of protection needed for virtualized mission-critical workloads.

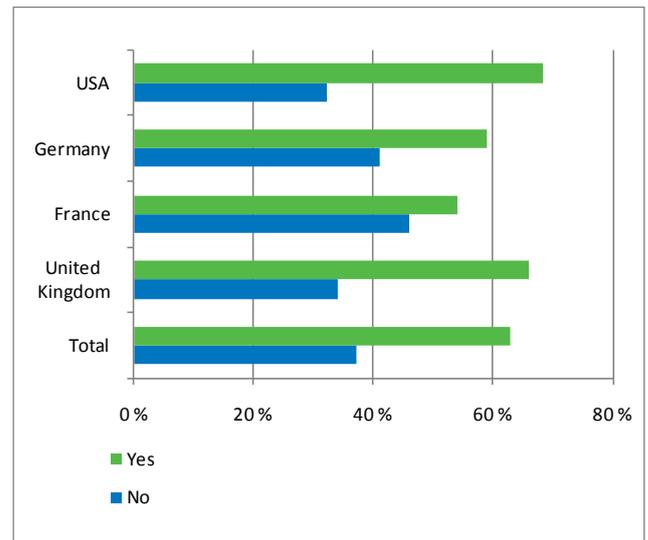


Chart 2.3: Percentage of enterprises that currently use a single product to back up BOTH physical AND virtual servers

Backup tools designed for physical servers are being used for virtual machines, but there are some limitations to this approach. Indeed, CIOs highlighted several shortcomings of using traditional tools for virtual machine backup of which the top three included high costs (51 percent), slow recovery (40 percent), and the need to install an agent (40 percent).

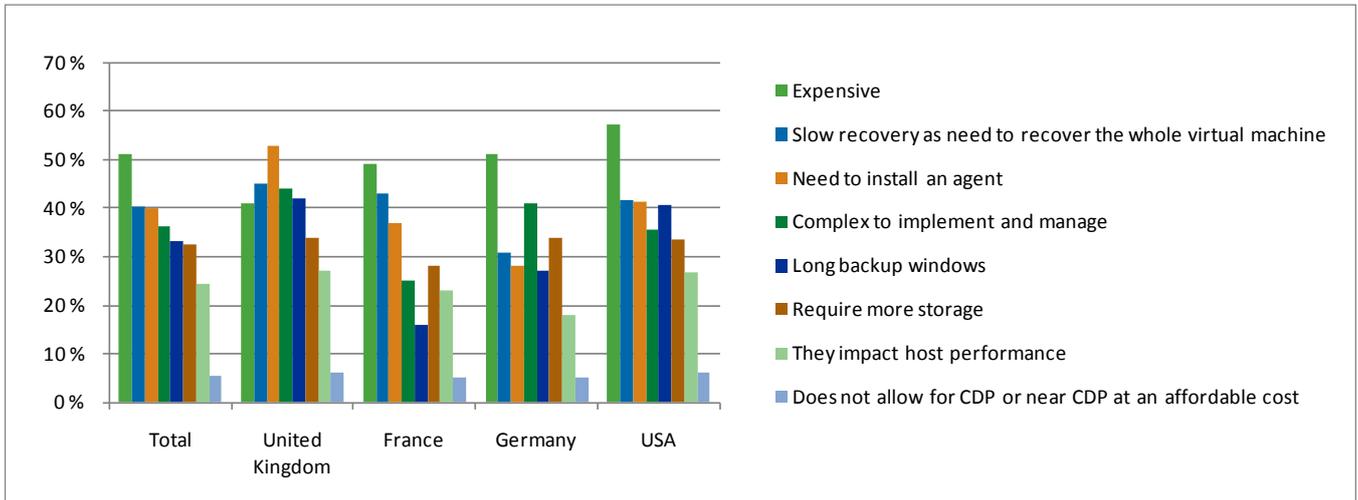


Chart 2.4: Shortcomings of traditional backup tools for use in virtualized environments

With traditional backup tools, performing standard recovery processes, such as a file-level restore from a backed-up virtual machine, requires IT departments to either recover the entire virtual machine first and then restore the individual file (38 percent) or keep two backups, one at a system level and another at

a file level (28 percent). These complicated restore methods stem from applying traditional backup strategies to virtual machines. Herein lies the core issue around virtualization and data protection. Simply put, enterprises today are using the wrong tool for the job.

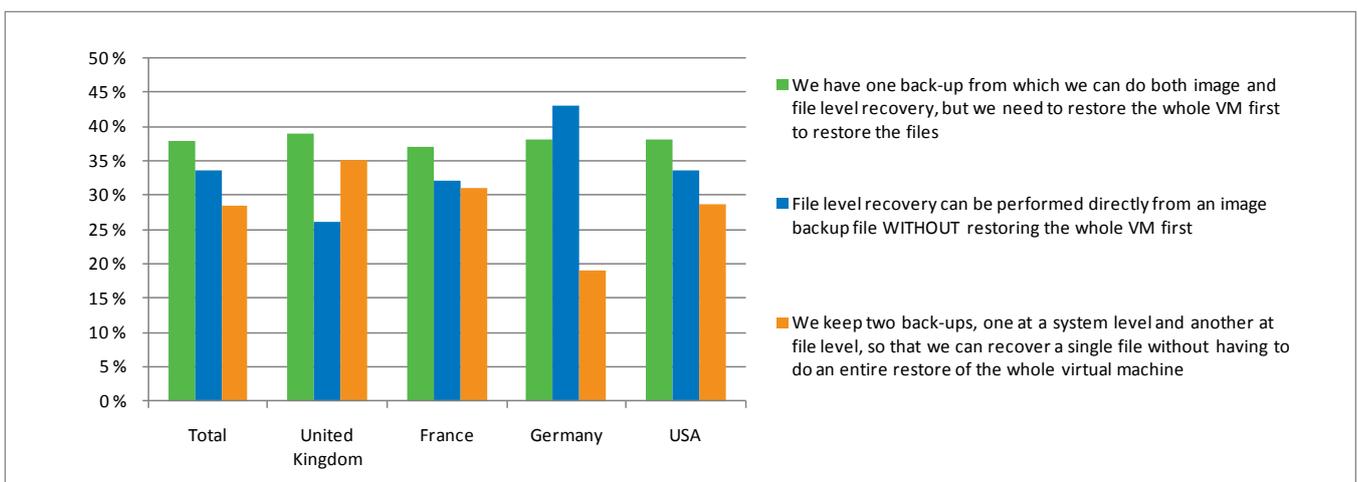


Chart 2.5: Approaches for recovering a single file from a virtual machine backup

Virtual Mindset

The challenge of using physical tools in the virtual world is a point that's being recognized. CIOs acknowledge that faster recovery (63 percent), faster backup (56 percent), and lower cost (54 percent) are their top reasons for deploying virtualization-specific backup tools.

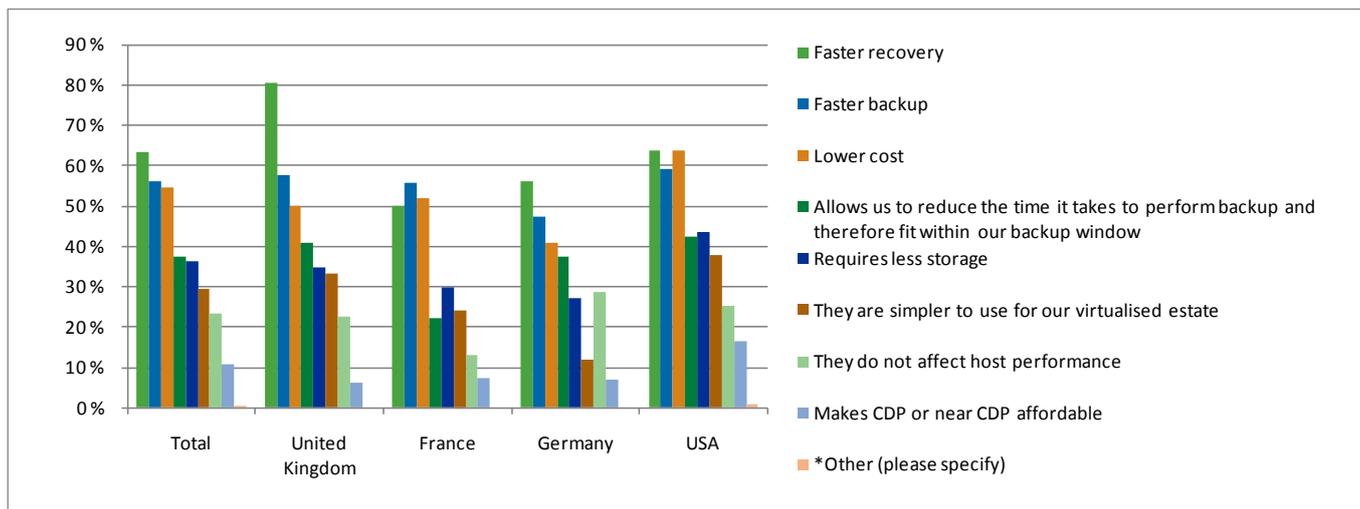


Chart 2.6: Benefits of deploying virtualization-specific solutions to back up virtual servers

Fifty-nine percent of businesses are now planning to deploy a virtualization-specific solution to back up virtual servers.

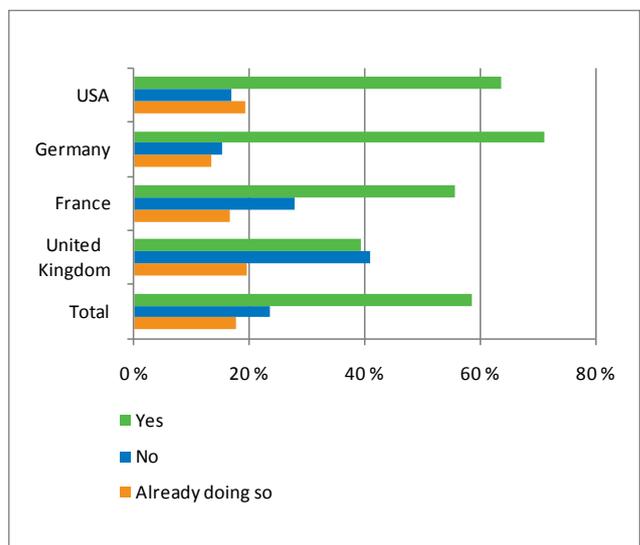


Chart 2.7: Businesses planning to deploy virtualization-specific solution for server backup and recovery

Sixty one percent will now also re-evaluate their data protection approach because of virtualization.

Breaking free from the physical world mindset and moving toward virtualization-based data protection requires a deep understanding of the new possibilities this technology brings. At a strategic level, a thorough review of existing policies and procedures must be undertaken. Problems that might previously have been thought impossible to address and therefore brushed under the carpet can now be addressed. More specifically, businesses should question exactly what has in the past been viewed as an acceptable level of risk and start to consider how this can be reduced, or even removed, by applying a virtual mindset.

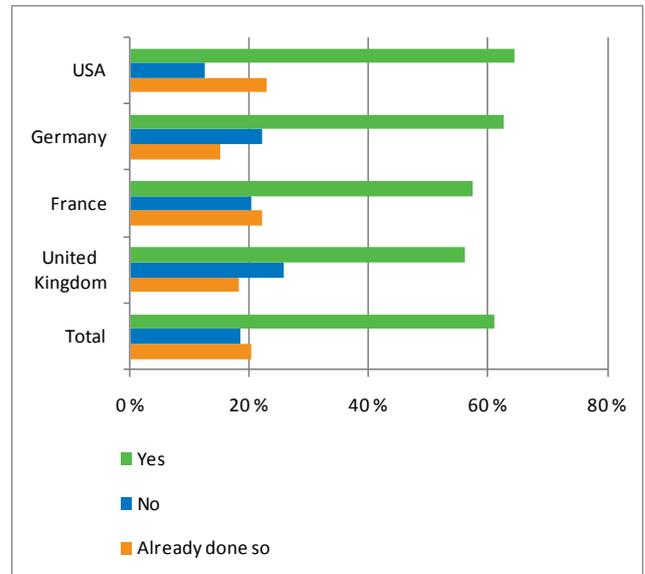


Chart 2.8: Businesses planning to re-evaluate data protection because of virtualization

Backup and Recovery Assurance

Data protection remains an ongoing challenge for businesses. In the past two years alone, nearly half (43 percent) experienced some form of data loss, which suggests there is much still to be done in this area.

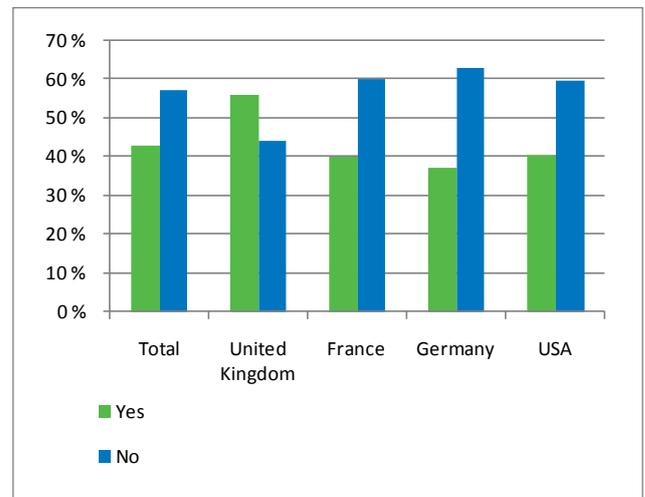


Chart 3.1: Percentage of organizations that suffered some form of data loss in the last two years

Continuous data protection (CDP) is seen as a way to improve data protection but most organizations agree it is too costly a solution to implement.

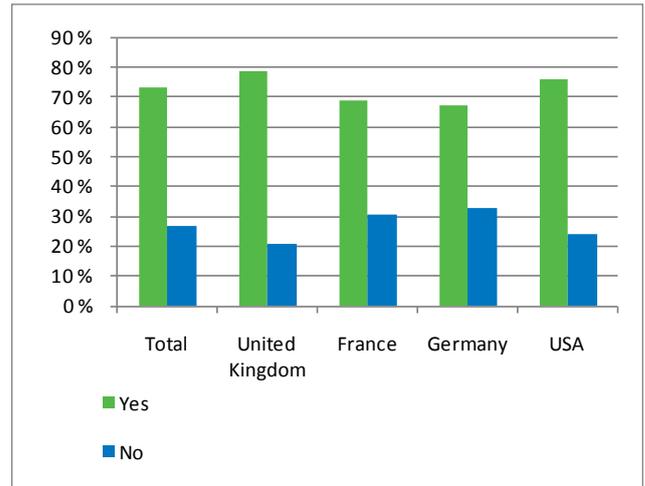


Chart 3.2: Percentage of organizations that use or would like to use continuous data protection (CDP) to improve disaster recovery plans and business continuity but don't because the cost of CDP is too high

More than half of all organizations are having to do the best with what they have as data protection budgets remain flat (45 percent) or decrease (15 percent) over the next two years.

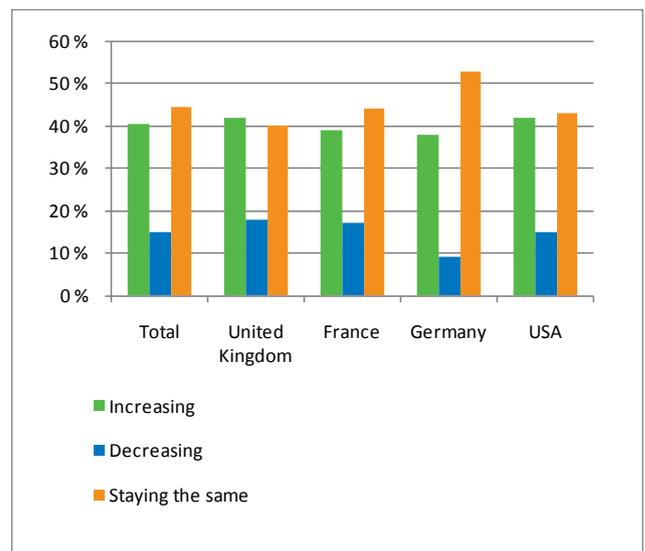


Chart 3.3: Data protection budgets over the next two years

Overcoming the Physical Mindset

Virtualization currently augments data protection strategies. For example, it is well understood that virtualization can reduce the physical server footprint in areas such as backing up data to off-site disaster recovery locations. However, the study showed that there is still a clear need for change in the area of backup and recovery assurance.

A major consequence of a physical IT mindset is that problems endured in this world continue to be seen

as acceptable risks. The recoverability of backup files is a problem that is as old as data loss itself. Organizations routinely need to recover servers and data. According to the research, hardware failure is the most common reason for backup recovery (experienced by 68 percent of organizations in the last year), closely followed by a general IT problem such as misconfiguration (63 percent), and user or operator error (56 percent) where someone accidentally deleted a file or object.

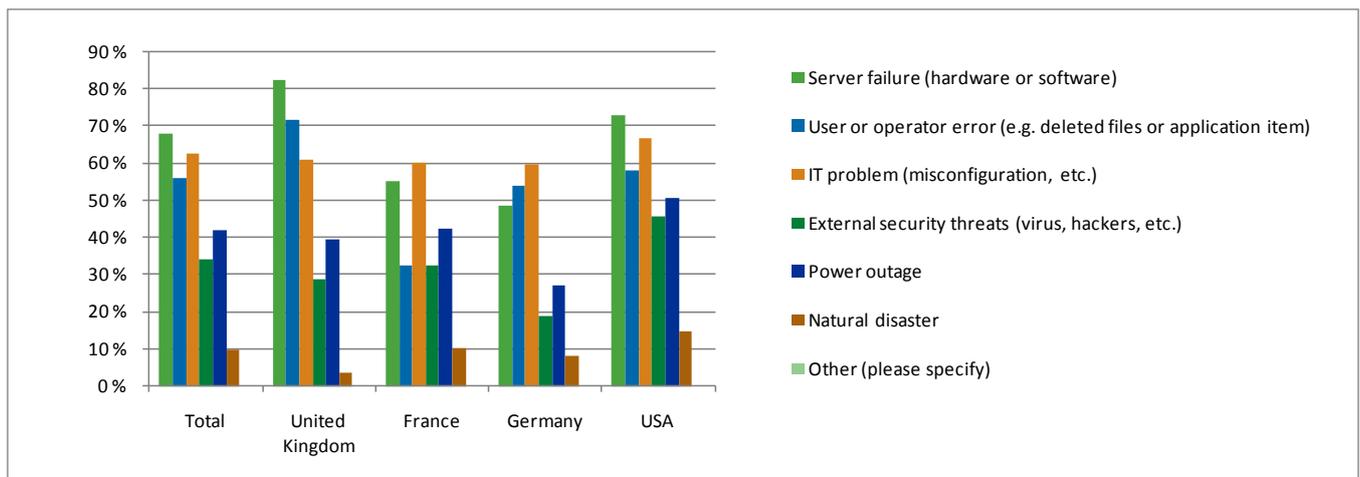


Chart 3.4: Scenarios leading to the need for data recovery

Unfortunately, nearly two-thirds (63 percent) of organizations experience problems every month when attempting to recover a server (be it physical or virtual).

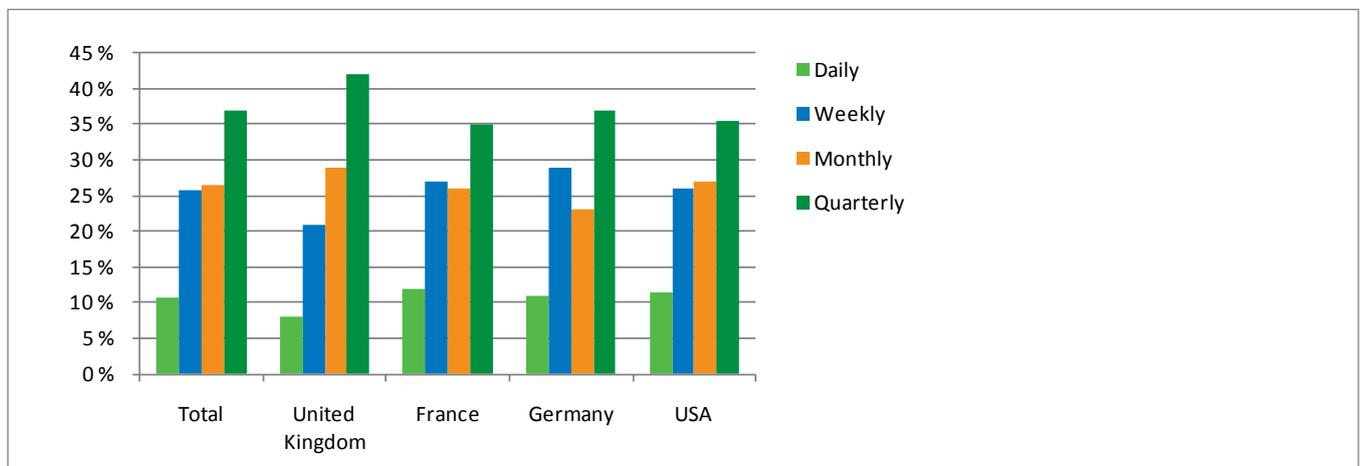


Chart 3.5 Frequency of problems when attempting to recover from a backup

Failed recoveries cost the average enterprise more than \$400,000 every year, highlighting how this problem appears to be a pain that businesses will live with.

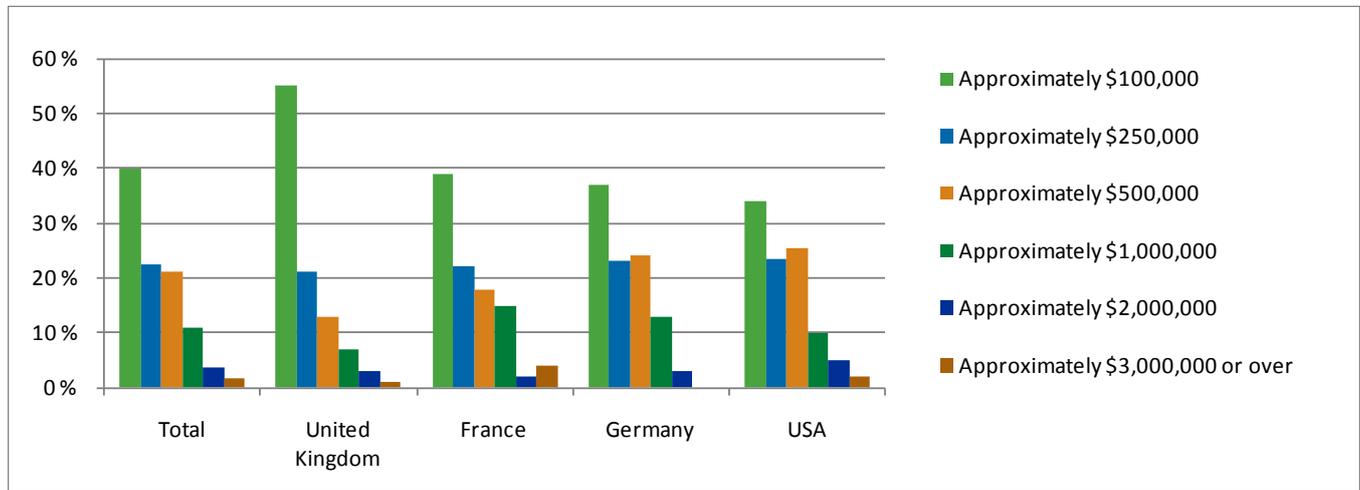


Chart 3.6 Cost of failed recoveries annually - note average = \$400,000

Testing Backups

On average, enterprises make 323,000 backups each year.

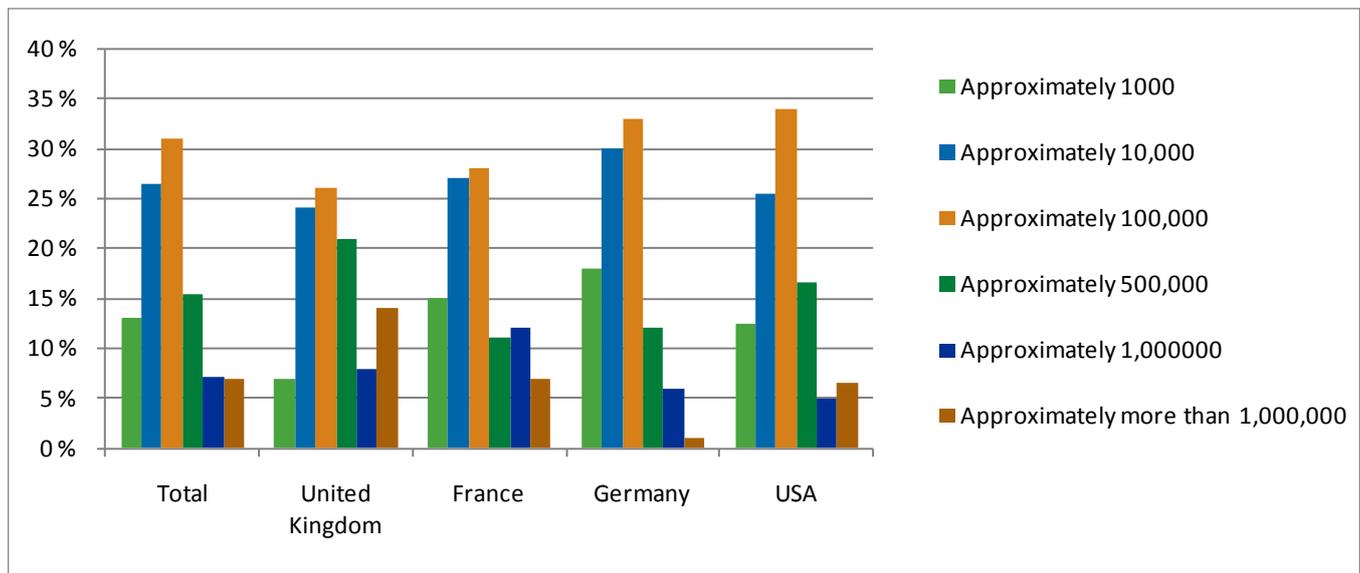


Chart 3.7: How many backups are made each year for all servers

Testing the recoverability of backups can help eliminate the problem of failed backups; however, only two percent of all backups are tested annually.

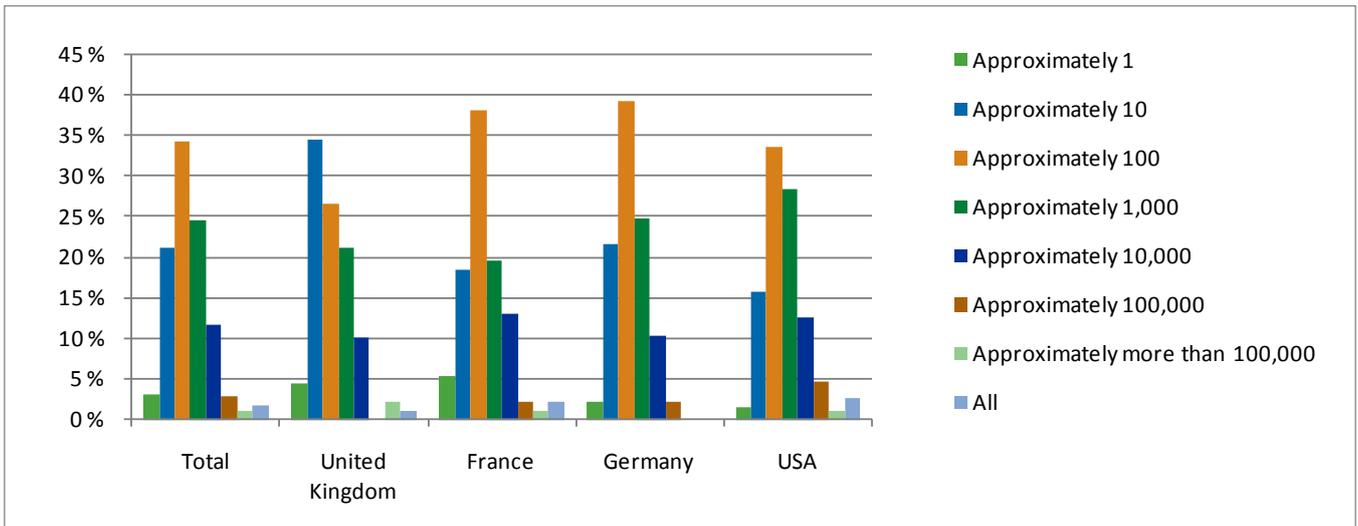


Chart 3.8: How many backups are tested for recoverability each year

On average backup tests are performed once every two months, leaving businesses with up to 60 days of bad backups.

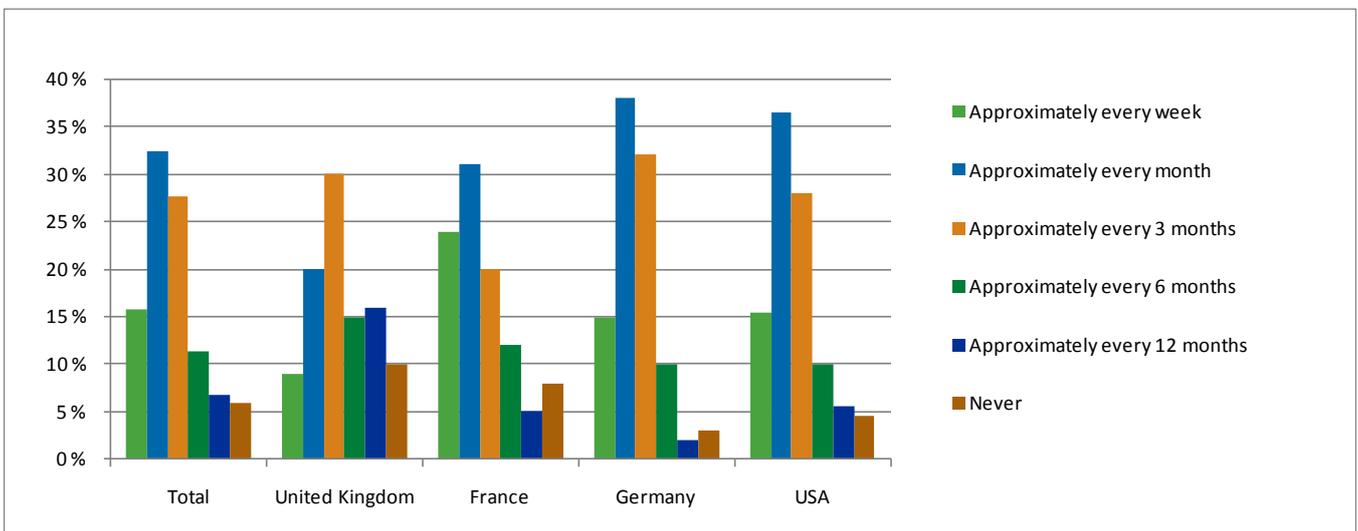


Chart 3.9: Frequency of backup tests performed - note average = 2 months

Respondents say testing the recoverability of a single backup takes IT teams an average of approximately 13 hours.

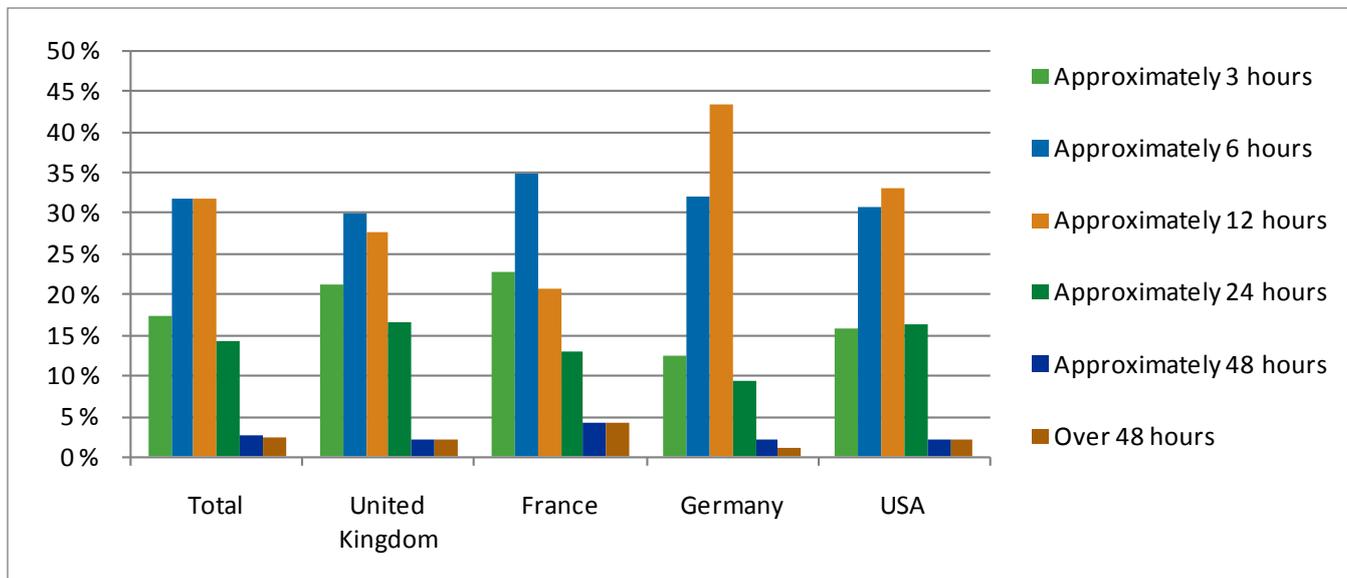


Chart 3.10: Amount of time required to test the recoverability of a backup

A lack of human resources is the top reason (61 percent) why IT departments do not test the recoverability of more backups.

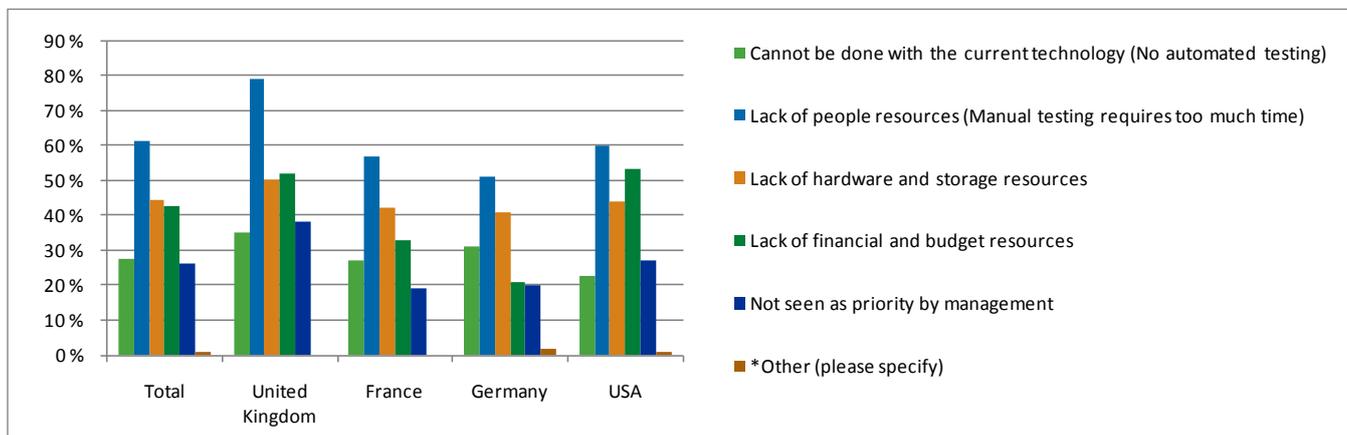


Chart 3.11: Barriers to testing the recoverability of every single backup

Recovery times

While it's widely accepted that a virtual machine can be built and deployed in minutes, CIOs indicated that on average, performing a full recovery of a backed up virtual machine still takes nearly five hours — a relatively small improvement in the six hours required to recover a physical server.

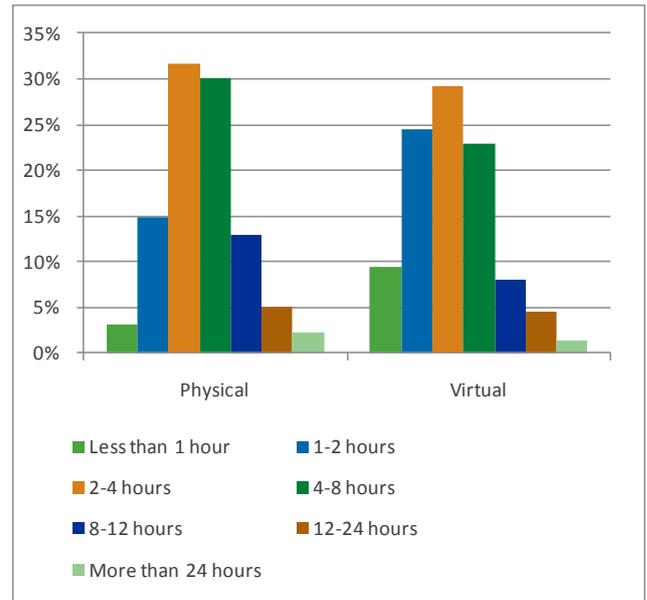


Chart 3.12: Comparison between physical and virtual server recovery times.

Note: Average for physical = 6 hours and virtual = 5 hours

With the proper tools, 25 percent of full server recoveries could be eliminated. Currently, 25 percent of such recoveries are being performed to recover a single file or application item. Moreover, 72 percent of all data recoveries involve granular recoveries of a file(s) or application item(s). This highlights the importance of using a backup product that offers a fast and simple way to recover files and application items from an image-based backup.

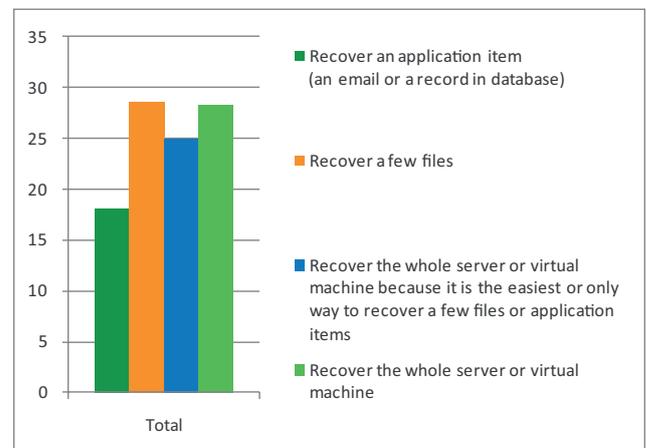


Chart 3.13: Scenarios of data recovery approaches

Thinking Beyond the Impossible

A major consequence of a physical IT mindset is that problems endured in this world continue to be seen as acceptable risks. However, the physical world limitations highlighted in this study are no longer applicable in the virtual world. In fact, with IT directors reporting that they plan to expand the use of virtualization in their server infrastructure from 42 percent to 63 percent during the next two years, businesses are in a much better position to finally address these issues if they deploy the right virtualization-based data protection strategies.

With the right tools, virtualization can make the impossible, possible.

Summary and Conclusions

CIOs often cite enhanced data protection as one of the primary reasons to virtualize, but the technology holds a huge amount of potential that businesses aren't currently tapping into. Although virtualization is improving IT costs and efficiency, this survey highlights how similar strides have not been made in data protection. The state of virtualization-based data protection today has revealed the following key insights:

- Virtualization is fast becoming a business-critical platform – moreover, it holds the potential to become the de facto platform for all IT infrastructure within the enterprise.
- Fears around data protection are a major barrier to increased adoption of virtualization in the enterprise.
- Businesses are recognizing that using traditional, physical backup and recovery tools for virtualization carries significant limitations and, subsequently, risks around data protection.
- Virtualization backup and recovery strategies are currently applied with a physical world mindset, but the right tools can transform the entire field of data protection.

About Veeam Software

Veeam Software is an innovative provider of VMware data protection, disaster recovery and VMware management solutions for virtual datacenter environments. This is the first annual report, and Veeam will continue to track the progress of enterprise strategies around virtualization-based data protection. Based on these findings, Veeam is optimistic about the maturity of this specific aspect of virtualization management. Through our industry-leading technology, we will evangelize the significance of Virtualization-Powered Data Protection.

In October 2010, Veeam released [Veeam Backup & Replication™ v5](#). This new version of Veeam's award-winning solution includes ground-breaking vPower™ technology for Virtualization-Powered Data Protection™. With five patents pending, [Veeam Backup & Replication v5](#) not only overcomes the limitations of traditional backup and recovery, but fundamentally transforms the market for data protection solutions.

vPower

vPower leverages virtualization and Veeam innovation to overcome the limitations of traditional backup and provide fast, flexible and reliable recovery for disasters both large and small. vPower includes the ability to run a virtual machine in production or in an isolated virtual lab directly from a compressed and deduplicated backup file on regular backup storage. As the force behind the [Veeam Backup & Replication v5](#), vPower offers five industry firsts:

- 1. Instant VM Recovery:** Restore an entire virtual machine from a backup file in minutes. Users remain productive while IT troubleshoots the issue. This massively reduces lengthy recovery times that respondents in the survey currently experience when recovering virtual machines. Recovery time objectives (RTOs) are improved from hours to minutes without additional cost.
- 2. U-AIR™ (Universal Application-Item Recovery):** Recover individual items from any virtualized application, on any operating system, without additional backups, agents or software tools. Eliminates the need for expensive special-purpose tools and extends granular recovery to all applications and users. This removes the current inefficient processes IT department have to undergo when recovering full virtual machines just to recover individual files and application items. It dramatically improves RTOs from hours to minutes for the most common recovery scenarios.
- 3. SureBackup™ Recovery Verification:** Automatically verify the recoverability of every backup, of every virtual machine, every time. Eliminates uncertainty and sets a new standard in data protection. The vast amount of time and resources needed to test backups are essentially removed in one go.
- 4. On-Demand Sandbox:** Create test VMs from any point in time to troubleshoot problems or test workarounds, software patches, or new application code. Eliminates the need for dedicated test labs and the overhead that extra VMware snapshots place on virtual machines.
- 5. Instant File-Level Recovery for any OS or file system:** Recover an entire VM or an individual file from the same image-level backup. Extends instant file-level recovery to all virtual machines.

100% Reliability	Best RTOs	Best RPOs
 SureBackup™	 InstantRestore™	 SmartCDP™
vPower™		
Virtualization-Powered Data Protection™		
5 Patents Pending!		
VMware vSphere		

Accelerating the Use of Virtualization

By using [Veeam Backup & Replication v5](#), IT departments can offer a much better service at a much lower cost. More importantly, Virtualization-Powered Data Protection offers businesses a solid foundation to virtualize more applications and accelerate the adoption of virtualization.