SMB edition

VEEAM
Modern Data Protection

Virtualization Data Protection Report 2013

Executive Summary

For the first time, the Virtualization Data Protection Report 2013 looks at the challenges that Small and Medium Businesses (SMBs) are facing with data protection strategies for their virtual environments. This year's report investigates whether organizations are confident in their data protection capabilities for their virtual environments. It identifies specific issues SMBs are experiencing with their virtual environments and suggests some of the underlying causes behind these. In particular, it highlights how capabilities, complexity and cost are key challenges for organizations of this size wishing to consistently protect their most critical servers and data. Currently, 85% of SMBs are experiencing issues around cost, 83% around capability, and 80% around complexity. Partly this is based on continued attempts to apply "traditional", physical-world based strategies to data protection in virtual environments, instead of adopting a more modern approach.

The report also demonstrates some of the actions organizations are taking to deal with the challenges they face in implementing data protection in their virtual environments. For example, 55% of SMBs plan to change their tools for backing-up virtual environments in the next 2 years.

The report has also uncovered a variation between the backup and recovery capabilities of SMBs of differing sizes. In general the larger an SMB is the less effective its backup and recovery was found to be, based on measurements such as the time to recover virtual servers or individual files and the proportion of the virtual infrastructure that can be backed up.

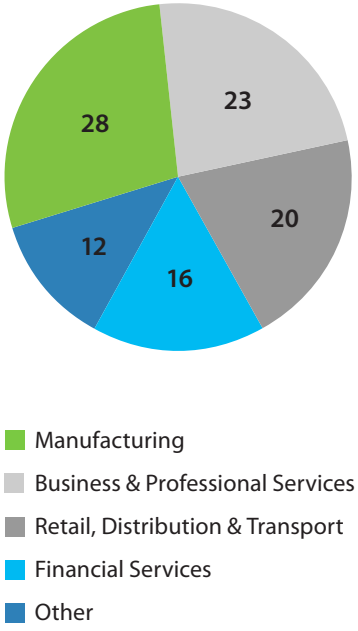
Finally, the report shows how modern virtualization-based data protection can help SMBs address a number of challenges that would otherwise be too costly or complex to tackle in a traditional manner. For example, 65% of SMBs surveyed believe that the costs of specialist e-discovery tools are prohibitively expensive: a problem that can be addressed by using modern data protection tools to identify and recover relevant emails and other files when necessary. There is also the technique of replication: which can be costly to implement traditionally, but is becoming rapidly more affordable with the use of virtualization and modern data protection tools.

The report is based on an online survey conducted in November and December 2012 by Vanson Bourne, an independent market research organization. It surveyed 500 CIOs or heads of IT from organizations across the United States, United Kingdom, Germany, and France that employ between 250 and 1,000 people. The report is sponsored by Veeam Software.

Survey Background

As in previous enterprise-level surveys, respondents came from a variety of industries. The most well represented field was Manufacturing (28% of respondents), followed by Business & Professional Services (23%), Retail, Distribution & Transport (20%) and Financial Services (16%). Other commercial sectors represented 12% of the survey sample. As a result, responses came from a range of SMBs across different sectors.

Chart A:
Types of organizations surveyed (%)



Part I | Cost Challenges for SMBs

1. Cost Challenges for SMBs

To begin with, 85% of SMBs are facing cost-related challenges with the backup and recovery of virtual servers. These direct costs cover three distinct areas: high ongoing management costs, affecting 51% of SMBs; expensive licensing models (48%); and backups either requiring or using too much storage (44%) (Chart 1). These issues are more pronounced for larger organizations: 90% of SMBs with 751-1,000 employees experience cost-related issues, compared to 84% of those with 501-750 employees and 78% of those with 251-500 employees. Since SMBs are often run on tight budgets, addressing these challenges is essential for ensuring data protection provides the best possible value for the business. Reducing management costs; providing easy-to-understand and low-cost licensing; and making backups as storage-friendly as possible, will be vital in this.

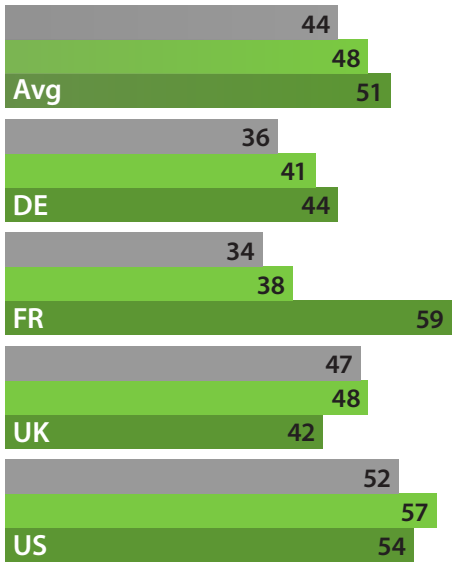


Chart 1: Cost-related challenges identified, %

Backups require too much storage
Expensive licensing models
High ongoing management costs

Part II | Capability Challenges for SMBs

2. Capability Challenges for SMBs

While direct costs may have been the most easily-identifiable challenge, 83% of SMBs identified capability-related challenges that are impacting their ability to backup and recover their virtual infrastructures. Again, these challenges were most pronounced in larger SMBs: 87% of those with 751-1,000 employees reported issues, compared to 83% of those with 501-750 employees and 78% of those with 251-500 employees. These illustrate a failure to realize the full potential of virtualization-based data protection. If used correctly, virtualization provides much higher data protection capabilities than a traditionally managed physical environment. With the right tools, entire virtual servers or individual files and application items can be recovered in a matter of minutes, allowing SMBs to recover quickly from disasters both large and small. This rise in efficiency, as well as the increased capability of modern data protection tools, means that SMBs can then focus on tasks that further improve data protection: for example, testing backups to ensure that they can be recovered when needed. By taking this approach, SMBs should be able to set and keep much more rigorous SLAs, and therefore be better placed to meet Recovery Point Objectives and Recovery Time Objectives, in turn improving the organization's ability to minimize IT downtime.

However, currently SMBs are not seeing a significant improvement in the performance of data protection for virtual environments. While recovery of physical servers takes, on average, 4 hours 54 minutes, recovery of virtual servers is only a little faster, at 4 hours 21 minutes (Chart 2). This again varies by size: those SMBs with 251-500 employees can recover their virtual servers in 3 hours 52 minutes, those with 501-750 employees in 4 hours 8 minutes and those with 751-1,000 employees in 4 hours 57 minutes: not significantly faster than the 5 hours 10 minutes it takes such SMBs to recover their physical servers.

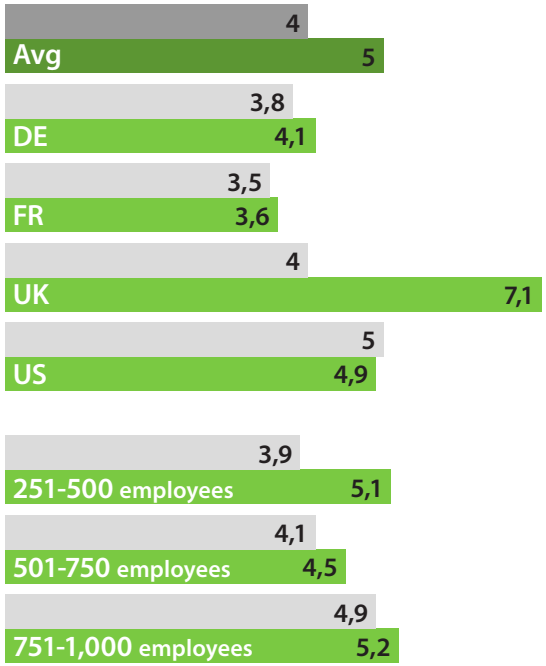


Chart 2: Time taken to recover backed-up servers (hours)

Time to recover virtual servers
Time to recover physical servers

Currently, 63% of SMBs feel that their backup and recovery tools will become less effective as the amount of data and servers in their infrastructure continues to grow (Chart 3): meaning that these recovery times may well increase over time. Perhaps unsurprisingly, larger SMBs are most concerned: 66% of those with 751-1,000 employees have these concerns, compared with 63% of those with 501-750 employees and 58% of those with 251-500.

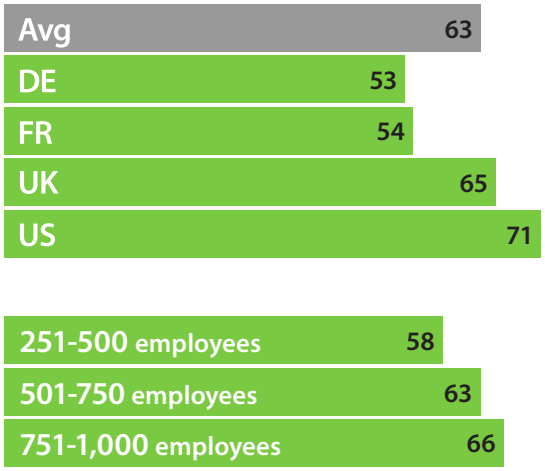


Chart 3: Organizations feeling backup & recovery will become less effective (%)

In terms of financial impact, 41% of SMBs stated that the cost per hour of downtime for their business critical servers that had not been protected by techniques such as replication was $150,000 or more (Chart 4). In conjunction with recovery times of 4 hours or more this means that, on average, an outage can cost these SMBs over $600,000, especially those larger SMBs whose recovery times reach 5 hours even for virtual servers. Given that SMBs are usually run on very tight budgets, losses of this size could well be crippling: reducing these costs as much as possible should be a high priority.

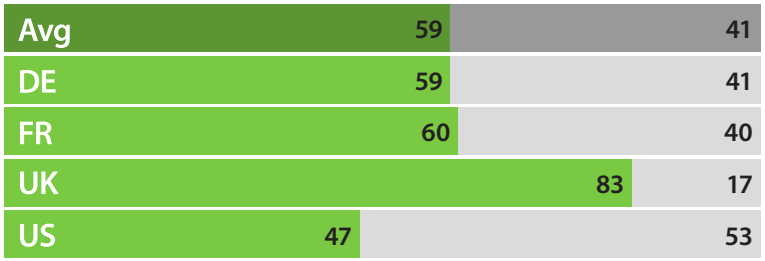


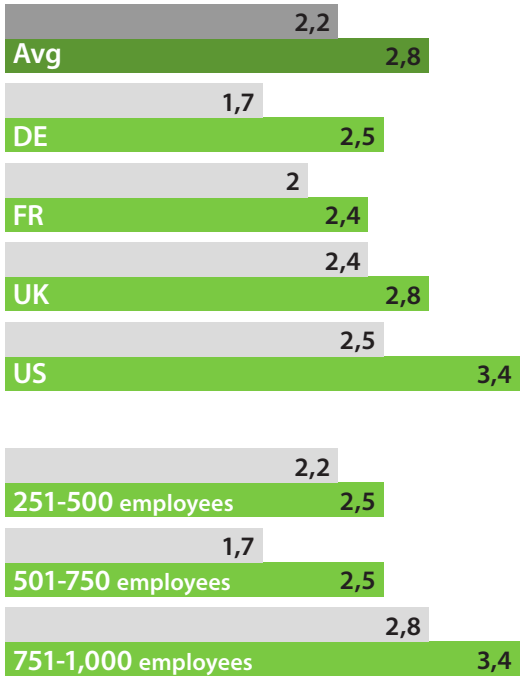
Chart 4: Cost-per-hour of critical servers being down (%)

Unreplicated servers costing $150,000 or more per hour of downtime

Unreplicated servers costing less than $150,000 per hour of downtime

SMBs will often require only certain application items or files to be recovered, rather than entire machines: the ability to do this means the SMB can operate in a more agile, and cost-effective manner. However, SMBs are still struggling with more granular recovery from virtual servers that should be more straightforward. On average, recovering individual files from a virtual server takes 2 hours, 21 minutes while application items take 2 hours 48 minutes to recover (Chart 5): while faster than recovering a whole server, this is still a significant wait and, again, is more pronounced for larger SMBs. Individual files take those with 751-1,000 employees 2 hours 50 minutes to recover, compared to 1 hour 40 minutes for those with 501-750 employees and 2 hours 12 minutes for those with 251-500. Even more pronounced, individual application items take SMBs with 751-1,000 employees 3 hours 22 minutes to recover. Those with 501-750 employees take 2 hours 32 minutes and those with 251-500 take 2 hours 28 minutes.

Certain items can be even slower: recovering individual emails takes an average of 12 hours 8 minutes (Chart 6). Again, the larger SMBs come off the worst: those with 751-1,000 employees take 14 hours 57 minutes, those with 501-750 11 hours 11 minutes and those with 251-500 employees 9 hours 56 minutes. These slow times are partly due to the fact that not all SMBs are able to perform granular-level recovery: 62% often have to recover more than they need in order to reach specific files or application items (Chart 7).



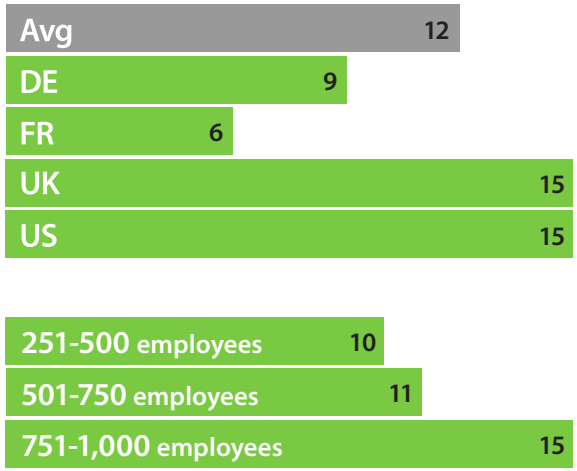


Chart 5 (on the left): Time to recover individual file or application items (hours)

Time to recover individual file from a virtual server

Time to recover indvidual application item from a virtual server

Chart 6 (on the right): Time to recover individual emails (hours)

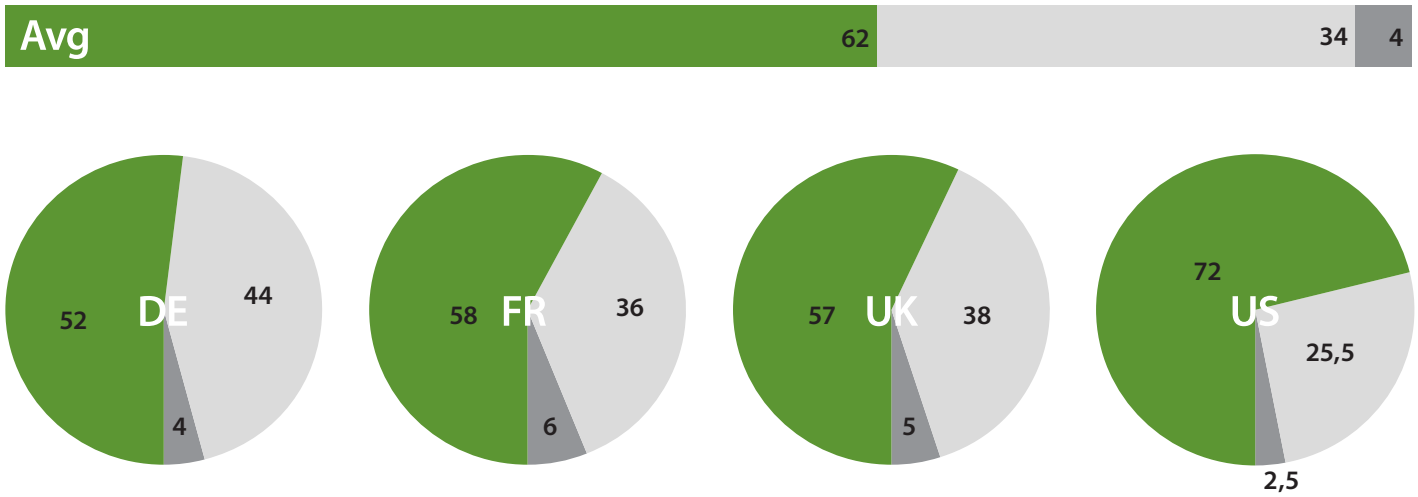


Chart 7: Organizations needing to recover more than desired to reach specific items (%)

- Organizations that often have to recover more than needed to reach specific items
- Organizations that can consistently recover individual items directly
- Organizations that do not offer the capability to recover individual files

This lack of granular recovery capability can have implications in a number of areas: for example, an SMB's ability to protect itself in the event of any legal challenges it faces. Traditionally, any legal challenge will require disclosure of all relevant documents: more and more this means that an SMB must be able to quickly discover, recover and present all relevant emails and files when required. However, the specialist e-discovery tools used for this are not aimed at the SMB market: 65% of SMBs feel that the cost of specialist e-discovery tools is prohibitively expensive (chart 8). Despite this, SMBs could rely less on e-discovery tools if they had confidence in their ability to quickly and accurately find and retrieve relevant items in the event of legal issues. With recovery of individual emails taking an average of 12 hours this is not the case. Reducing this timescale would provide SMBs with a cost-effective alternative to e-discovery on top of other backup and recovery capabilities.

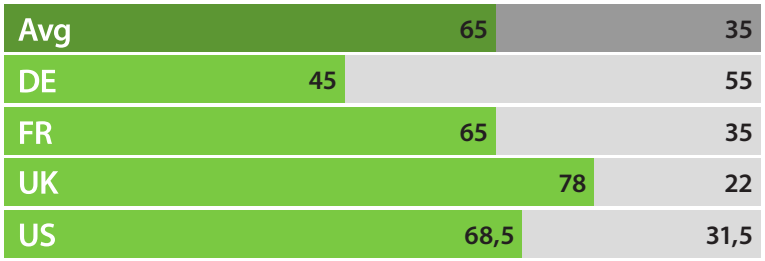


Chart 8: SMBs that find the cost of specialist e-discovery tools prohibitively expensive (%)

- Percentage of SMBs that do not find the cost of specialist e-discovery tools prohibitively expensive
- Percentage of SMBs that find the cost of specialist e-discovery tools prohibitively expensive

Regardless of time taken and granularity of recovery, SMBs also demonstrate issues guaranteeing the recoverability of backups. On average, SMBs experience problems when attempting to recover from backups 8 times per year (Chart 9). This accounts for 17.43% of all recoveries, meaning that the chances of an unsuccessful recovery are more than 1 in 6 (Chart 10).

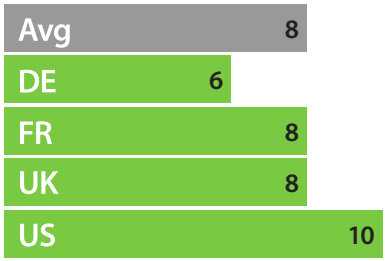


Chart 9: Number of times per year organizations experience problems attempting to recover from backups

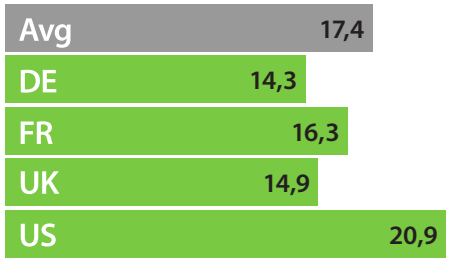


Chart 10: Percentage of recoveries that present problems (%)

A lack of opportunities to test backups may be one reason why the chance of problems with backups is so high. Currently, SMBs test their backups for recoverability every 3 months (Chart 11). However, on these occasions they only test on average 7.65% of all backups (Chart 12). Again, larger SMBs do not perform as well: those with 751-1,000 employees only test 6.36% of all backups, compared to 7.35% for those with 501-750 employees and 9.62% for those with 251-500. As a result, in any year there will be a large number of backups that remain untested. While SMBs can concentrate on the most critical areas, this still represents a large proportion that cannot be guaranteed, in turn making it harder for SMBs to confidently predict their availability SLAs.

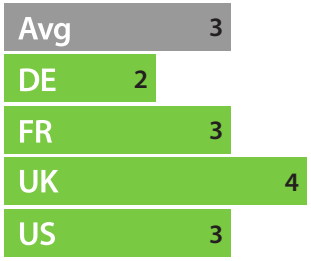


Chart 11: Frequency of backup testing (in months)

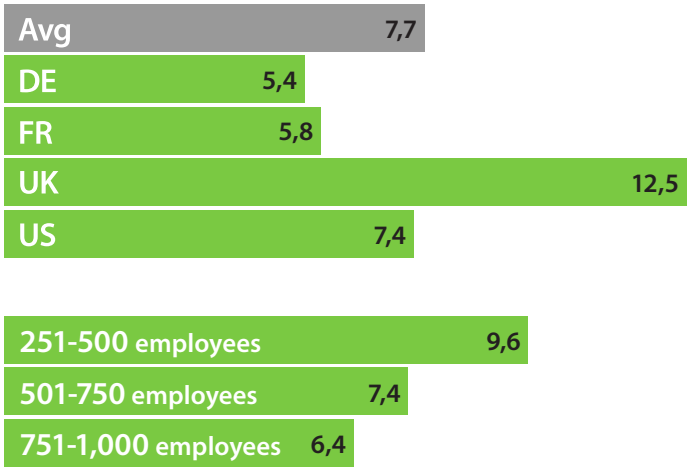


Chart 12: Percentage of backup servers tested when testing for recoverability (%)

As shown, there are significant capability-based challenges facing SMBs. However, SMBs must also recognize that they face these challenges. While an average of 83% admitted to facing capability-based issues, 40% stated that backup takes too long, while recovery taking too long was an issue for 34%. This suggests that 66% of SMBs do not believe they have an issue with their recovery times: given the average recovery time of 4 hours, it may be that SMBs are unaware of the true backup and recovery performance virtualization can offer. Alternatively, consistently using legacy tools better suited to a physical environment may have caused them to accept this level of performance as the norm. Beyond this, 25% of SMBS had difficulty recovering virtual servers, 23% stated that it was difficult to create or maintain backup jobs, 22% said that file- and application-level recovery was too difficult, and 18% that backup or recovery often fails (Chart 13). This again suggests either that SMBs may be unaware of any issues with these tasks or that they have become used to the relatively poor performance of their existing backup and recovery tools, given the recovery times and frequency of backup and recovery failure referenced above.

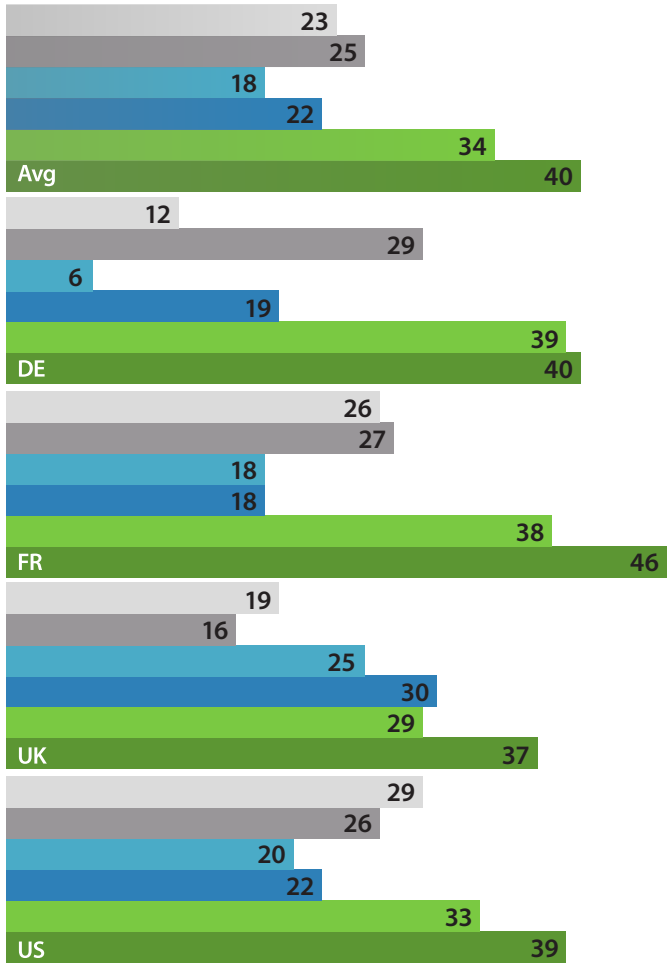


Chart 13: Capability-related challenges identified (%)

- Difficult to create or maintain backup jobs
- Dififcult to recover virtual servers
- Backup or recovery often fails
- File- and application-level recovery too difficult
- Recovery takes too long
- Backup takes too long

Also of note is how the larger SMBs consistently see lower performance of their backup and recovery capabilities, particularly in areas such as recovery time and the ability to consistently test backups. This may be down to the size of their infrastructure: while SMBs of all sizes are likely to have limited resources, a smaller SMB will have a correspondingly smaller IT environment meaning that its mission-critical servers which must be tested will form a larger proportion. At the same time, this smaller infrastructure and smaller amounts of data will make it easier and faster to identify and recover specific items.

Part III | Complexity Challenges for Organizations

3. Complexity Challenges for Organizations

Finally, 80% of SMBs said that they are experiencing complexity-related challenges with backup and recovery of virtual environments. These are again related to size: 85% of SMBs with 751-1,000 employees experience these challenges, compared to 79% of those with 501-750 employees and 74% of those with 251-500. In turn, these challenges will add to the total cost of virtual data protection and if not addressed could reduce its capability. Among these challenges are backups needing ongoing management (experienced by 52% of SMBs); too many virtual servers to backup (35%); backup tools being difficult to configure and use (32%); and difficulty backing up to tape (27%) (Chart 14). Modern data protection tools that can automate management, scheduling and configuration of backups, as well as using virtualization to remove the need for tape-based backup libraries, can be a huge help with these issues.

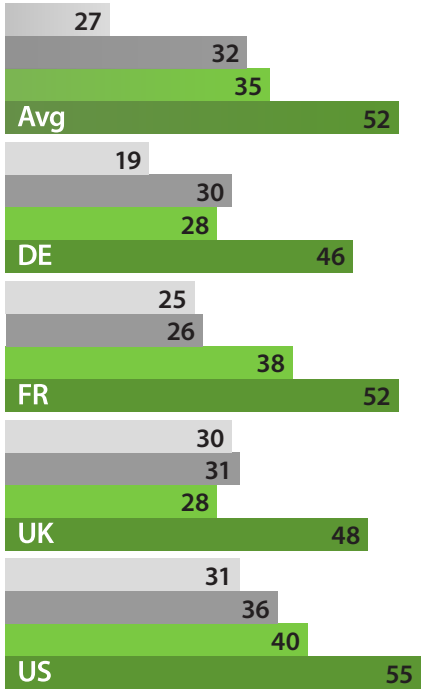


Chart 14: Complexity-related challenges identified (%)

- Difficulty backing up to tape
- Backup tools difficult to configure and use
- Too many virtual servers to backup
- Backups need ongoing management

In terms of technological approaches that can increase complexity, a significant difference between legacy backup tools and more modern approaches is the use of software agents on protected machines to make backup and recovery possible. By requiring agents to be installed, monitored and updated, agent-based backup can add extra layers of complexity to data protection: in turn making it easier to miss SLAs and increase costs. In a virtualized environment, agents can be done away with. This in turn removes the extra layer of management, making the process more cost-effective, faster, and less complex for the IT team.

Currently, 67% of SMBs surveyed say that their backup tool requires agents inside virtual servers. In turn, 76% of these experience problems or management issues due to agents: this represents 51% of all organizations surveyed (Chart 15).

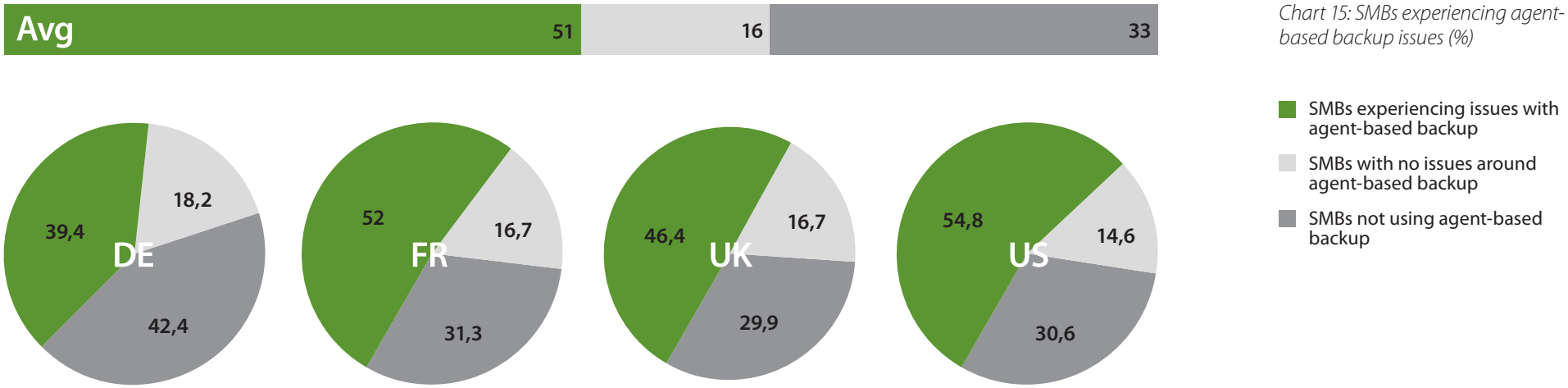


Chart 15: SMBs experiencing agent-based backup issues (%)

Common problems and challenges for those SMBs using agent-based backup and recovery include: agent management, for example installation, upgrading, updating and managing conflicts, which affects 43%; backups failing far too often (32%); the expense of agent-based backup (27%); restores failing too often (25%); and agents slowing down system performance (20%) (Chart 16). Based on these statistics there will be a relatively large number of SMBs experiencing multiple issues with agent-based data protection, in turn increasing the cost and complexity and reducing the capability of their backup and recovery strategy while increasing the chances of missing SLAs.

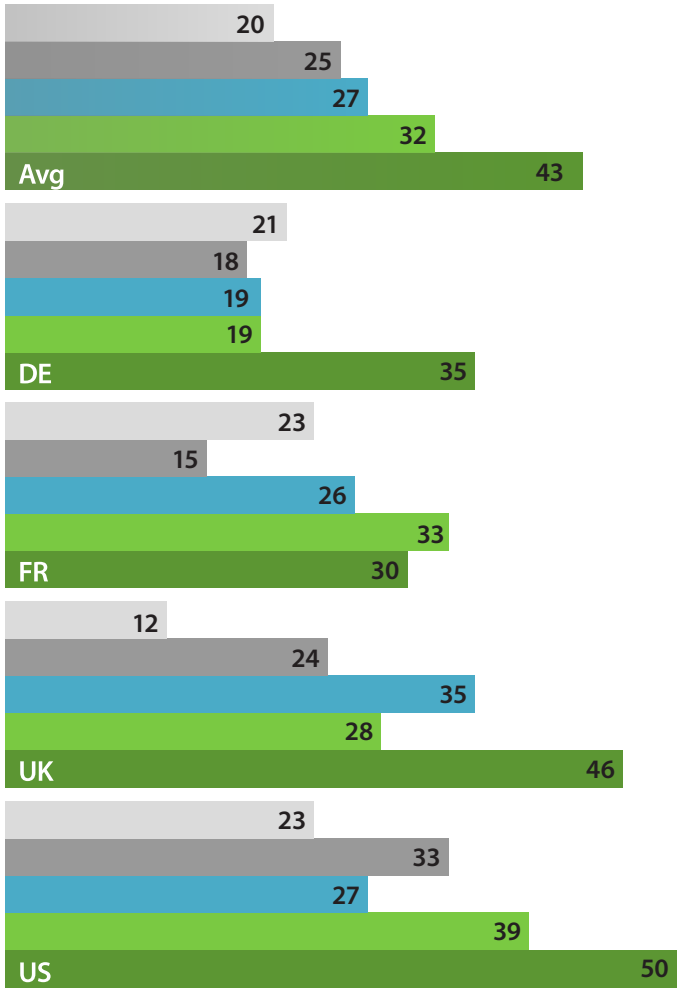


Chart 16: Agent-based backup issues identified

- Agents slowing down system performance
- Restores failing too often
- Expense of agent-based backup
- Backups failing too often
- Agent management

The survey also suggests that SMBs may be unaware that legacy, agent-based data protection tools are not necessarily the best possible option for a virtual environment. While half of the SMBs surveyed are experiencing issues that can significantly affect performance, 48% believe that it is better if a backup tool uses agents to aid backup and recovery. A further 24% believe that agent-based and agentless tools will work equally well for their needs (Chart 17). As the potential that modern data protection tools present becomes more commonly known, we would expect this to change: essentially, organizations will recognize those issues that are caused by agent-based data protection tools and begin to favour modern, agentless data protection tools that enable the setting of far more rigorous SLAs.

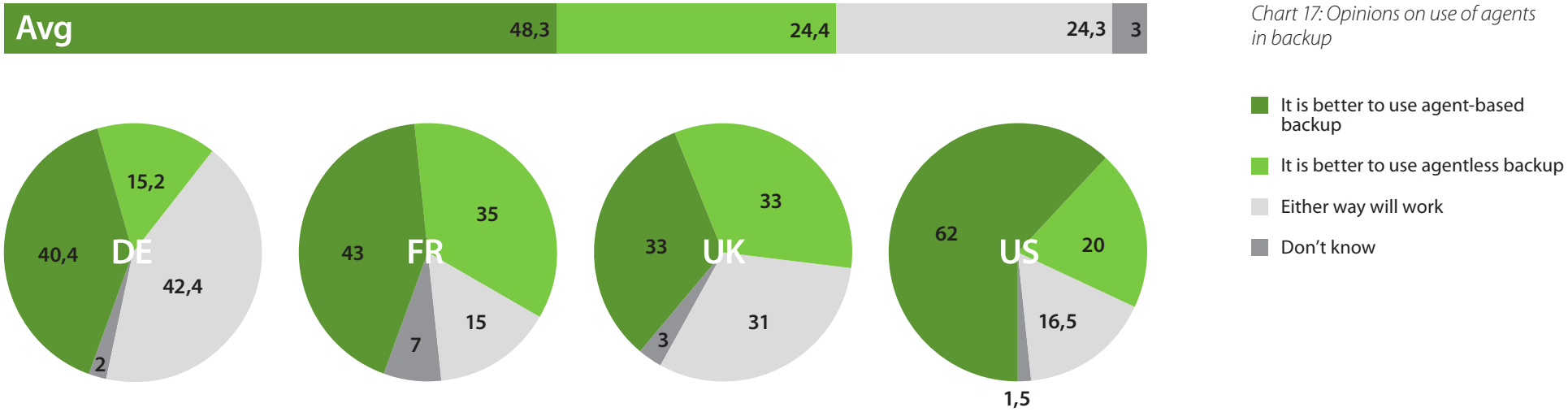


Chart 17: Opinions on use of agents in backup

Part IV | Potential Upheaval in the SMB Data Protection Market

4. Potential Upheaval in the SMB Data Protection Market

As we have seen, there are significant issues with data protection in the virtual environment. SMBs are experiencing issues with the base cost of their data protection tools, from management to licensing to the additional infrastructure required. The capabilities offered by many backup and recovery tools, especially legacy tools retrofitted to work with virtual infrastructures, are still not at the level that should be expected of the technology, resulting in missed or unambitious SLAs. And complexity challenges, along with the extra issues that use of agent-based tools can cause, are further adding to the cost and difficulty of implementing data protection strategies.

However, there are signs that SMBs are recognizing this and planning to change the way in which they work. Currently, 55% of SMBs are planning to change their backup tool for virtual servers in the next 24 months (Chart 19): those with 751-1,000 employees are most likely to change, with 62% planning on switching tools. On average, the expected time until a change is in fact only 10 months (Chart 20). This suggests that by 2014 a large proportion of SMBs will have fresh backup and recovery tools in place that may improve on a number of the issues above.

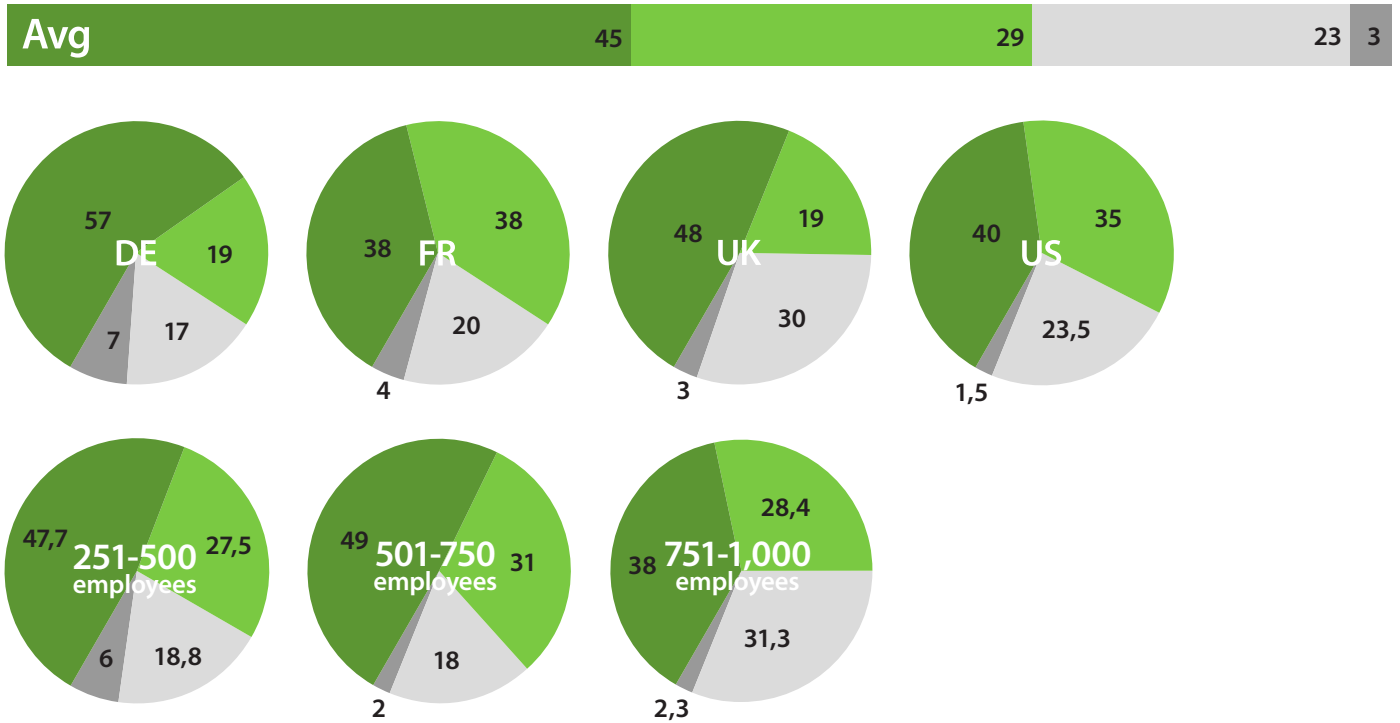


Chart 19: SMBs' plans to change backup & recovery tools

- No plans to change
- Planning to change within 6 months
- Planning to change within 12 months
- Planning to change within 24 months

Chart 20: Average timescale for changing backup tool (months)

Those SMBs planning to change their current tools cite a number of reasons around cost, complexity and capability. The most common reason given is Total Cost of Ownership, including management and maintenance (46%). Also high is complexity (44%), while the software and hardware costs of their current tool are reasons for 43% of these SMBs to change. Some SMBs cite lack of capability behind other reasons for changing: a failure to meet Recovery Time Objectives (30%) and Recovery Point Objectives (21%) are both given (Chart 21).

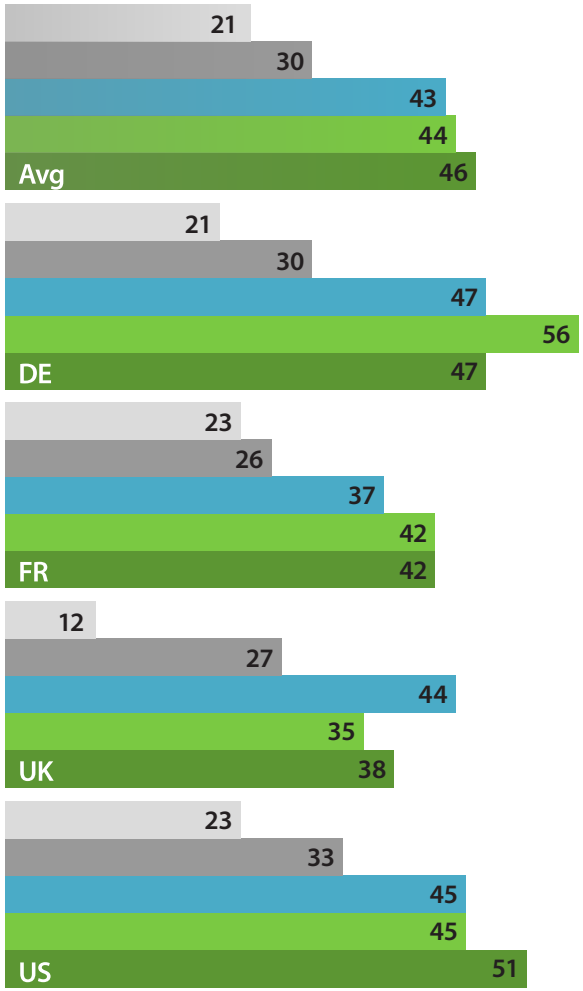


Chart 21: Reasons for changing current backup tool (%)

- Failure to meet Recovery Point Objectives
- Failure to meet Recovery Time Objectives
- Software and hardware costs
- Complexity
- Total Cost of Ownership

As we can see, cost, complexity and capability challenges are becoming increasingly important to SMBs: so important that they are driving their data protection strategies for the next 2 years. This may increase as more businesses become aware of the limitations behind legacy data protection tools.

Appendix

Appendix 1: The State of Virtualization Data Protection in the SMB

As server virtualization continues to grow in popularity, it is becoming an ever-more important part of the SMB IT infrastructure. Indeed, virtualization is now the dominant means of providing that infrastructure. This in turn provides new opportunities and challenges for SMBs. To begin with, there is still the decision of what infrastructure to protect, and to what extent. A virtual environment is potentially much easier to backup and recover than a physical one: as a result, SMBs have the capability to protect more of their infrastructure than ever before, while using fewer resources and at an ultimately lower cost.

Currently, on average 52.02% of the production server estate is virtualized in SMBs: within the next 2 years, this proportion is expected to grow steadily to 63.44% (Chart 22).

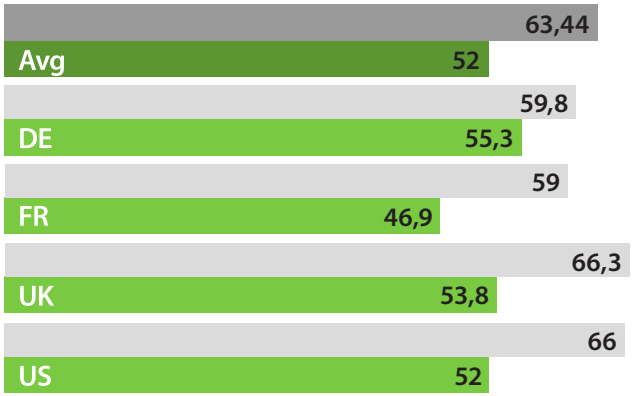


Chart 22: Current and predicted virtual estates (%)

Percentage of production server estate predicted to be virtualized in 2 years

Percentage of production server estate currently virtualized

When backing up their virtual environments, SMBs will generally use one of three approaches. The first is to use native tools that are part of their applications or operating system: these have the advantage of no additional costs beyond licensing the application or OS itself, but will tend to have limited awareness of virtualization compared to specialist data protection tools. Second, SMBs can use a single third-party tool to backup both their physical and virtual environments: this will allow an SMB to continue using its legacy backup solutions. However, those legacy solutions will not have been designed to backup and recover virtual environments; meaning the cost-saving will be offset by a lack of performance. Finally, SMBs can use separate specialist tools to backup their virtual environments. While such tools are relatively new they can exploit the nature of virtualization to provide the best possible performance and capabilities such as replication and e-discovery equivalents.

While virtualization is growing in popularity, the majority of SMBs are not backing up every single virtual server. 76% of SMBs do not backup 100% of their virtual servers (Chart 23). On average, all SMBs surveyed backup 67.17% of their virtual environment (Chart 24): while this is good, there is still the potential to reach into the remaining 33%.

Again, there is a pronounced difference between different sizes of SMB. Those with 751-1,000 employees backup 62.93% of their environment, with 15% backing up 100%. SMBs with 501-750 employees backup 69.60% of their environment, with 24% backing up 100%. Lastly, those with 251-500 employees backup 69.38% of their environment, while 33% backup 100%. Again, this may be down to the size of the infrastructure: smaller SMBs with smaller infrastructures will find it correspondingly easier to backup 100% with limited resources.

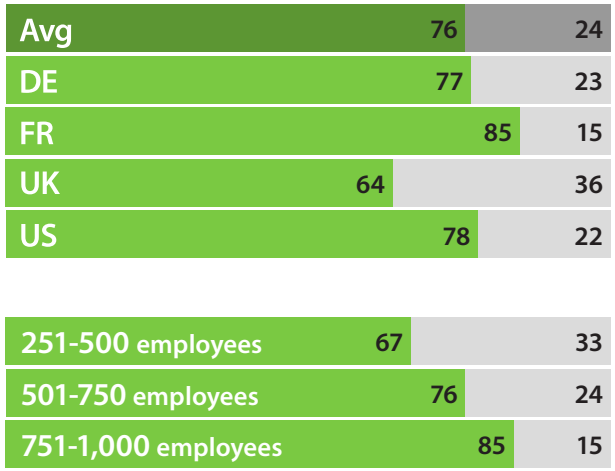


Chart 23 (on the left): Percentage of Organizations protecting 100% of virtual servers (%)

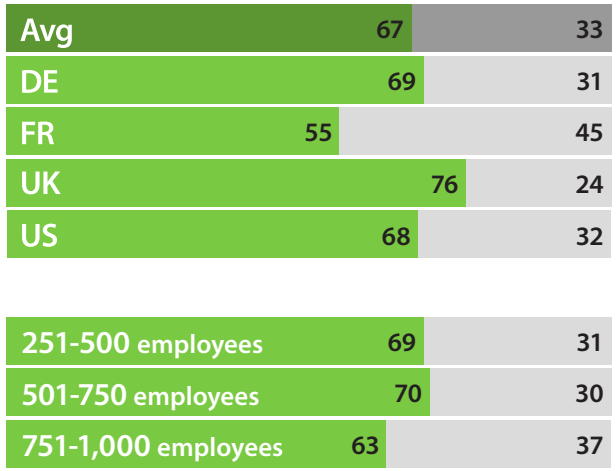


Chart 24 (on the right): Percentage of virtual infrastructure protected (%)

- Protect 100% of virtual servers
- Do not protect 100% of virtual servers

- Percentage of virtual infrastructure protected
- Percentage of virtual infrastructure unprotected

SMBs are divided on the tools they use to backup their virtual environments. 7% use native tools to backup their virtual servers. 56% use a single third-party tool to backup both physical and virtual servers. 37% use a specialized tool for their virtual environments (Chart 25). This suggests that SMBs are still most comfortable using legacy tools to protect their virtual environments, rather than investigating more modern solutions. However, as specialist tools are still relatively new we would expect this to change over time.

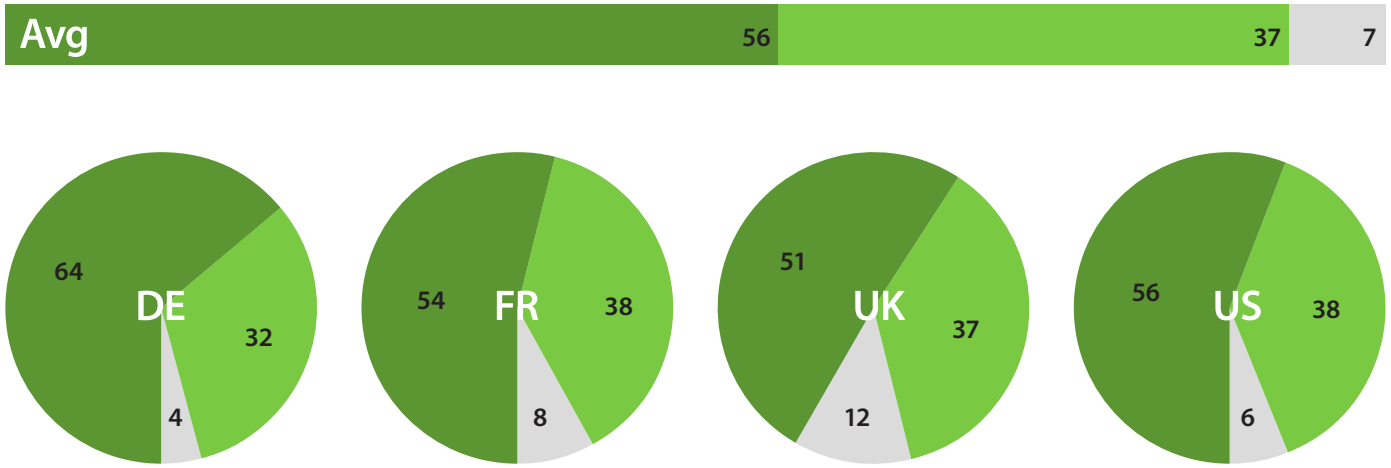


Chart 25: Tools used for data protection (%)

Appendix 2: Use of Replication

One capability made more accessible through virtualization in conjunction with modern data protection tools is replication. Replication is typically a process of copying data to production standard hardware that can be brought back online quickly in the event of a data loss. This differs from the process of 'backup', whereby data is basically compressed and then stored on relatively inexpensive hardware. In the event of data loss, this must first be restored before it can be brought back online.

Server replication has traditionally been a cost- and resource-intensive process, especially as most replication solutions must be purchased separately to backup tools: this in turn has placed it beyond the grasp of many SMBs. While virtualization can help make replication less costly, for example by enabling more efficient creation of the required infrastructure, its use is not yet universal. Currently, 69% of SMBs use replication to some extent: 42% using hardware-based and 27% using software-based (Chart 26).

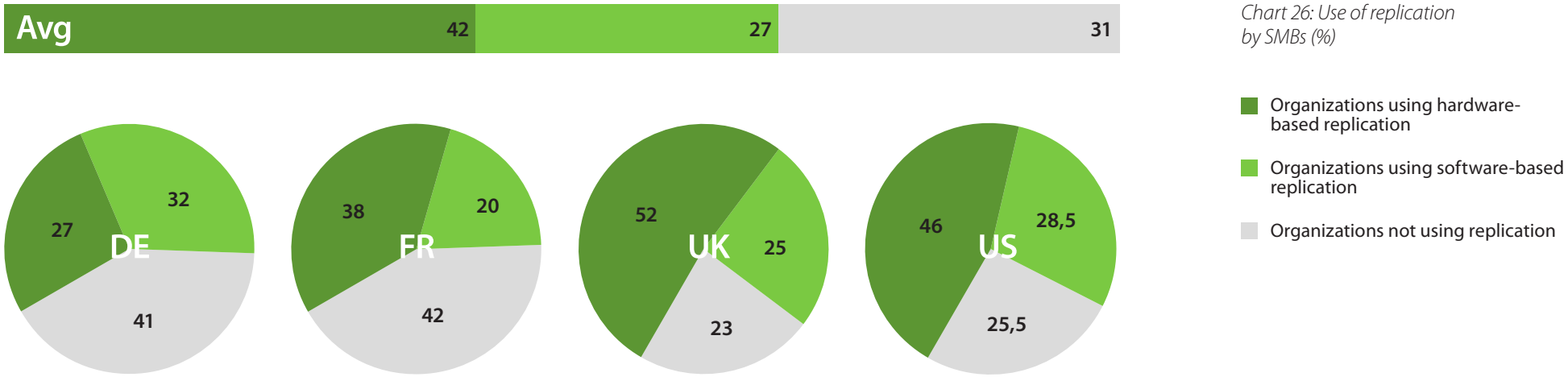


Chart 26: Use of replication by SMBs (%)

However, replication has a clear cost benefit for SMBs that can use it. Replicated servers would cost $359,475 per hour of downtime if they were not so protected (Chart 27). Given the average time to recover a server of at least 4 hours, we can see that those SMBs using replication are essentially saving themselves over $1.4 million each time they need to make use of their replicated infrastructure. With the established financial pressures that often affect SMBs, this can have an exponential value to the business.

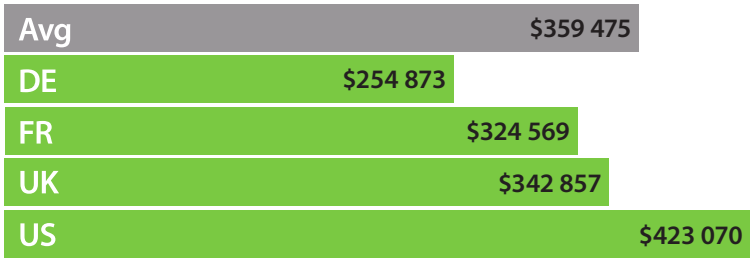
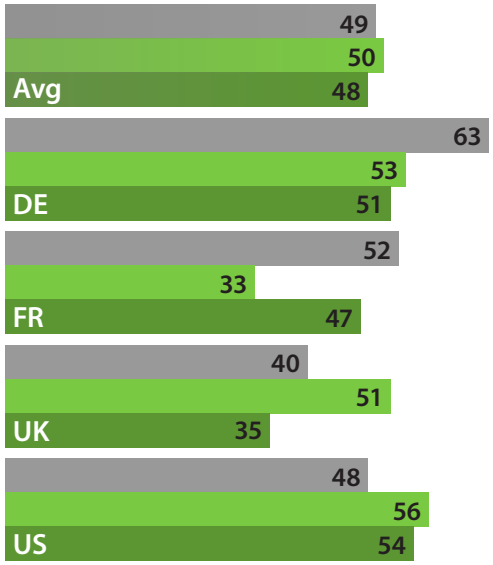


Chart 27: Cost-per-hour of replicated servers being down (USD)

It seems natural that SMBs should want to adopt replication, especially as virtualization and modern data protection tools make it more affordable. However, there are still barriers to increased use. The top 3 barriers for SMBS are the cost of replication hardware (50%), complexity (49%), and the cost of software (48%) (Chart 28). For those SMBs that have yet to adopt replication the reasons given focus on cost: whether hardware (52%) or software (52%). The next most common concern is again complexity, although this is only for 38% of SMBs (chart 29).



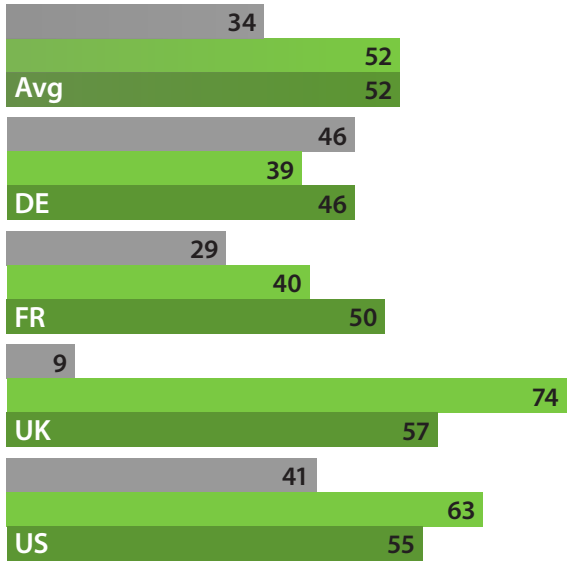
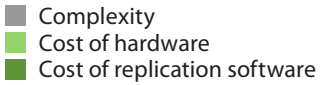
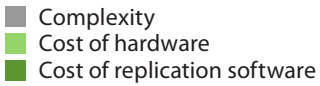


Chart 28 (on the left): Issues preventing greater use of replication (%)

Chart 29 (on the right): Issues preventing adoption of replication (%)





About Veeam Software

Veeam® Software develops innovative solutions for VMware backup, Hyper-V backup, and virtualization management. Veeam Backup & Replication™ is the #1 VM Backup solution. Veeam ONE™ is a single solution for real-time monitoring, resource optimization, documentation and management reporting for VMware and Hyper-V. Veeam extends deep VMware monitoring to Microsoft System Center with Veeam Management Pack™ (MP), and to HP Operations Manager with Veeam Smart Plug-In™ (SPI). Veeam also provides free virtualization tools. Learn more by visiting www.veeam.com.

Virtualization changes everything – especially backup. If you've virtualized on **VMware** or **Hyper-V,** now is the time to move up to the backup solution Built for Virtualization: Veeam.

Unlike traditional backup that suffers from the **"3C" problem** (missing capabilities, complexity and cost), Veeam is:

- **Powerful:** Restore an entire virtual machine (VM) or an individual file, email or database record in 2 minutes
- **Easy-to-Use:** It just works!
- **Affordable:** No agents to license or maintain, works with your existing storage, and includes deduplication, VM replication, Microsoft Exchange recovery, and more

Join the 60,000 organizations who have already modernized their data protection with Veeam.
Download Veeam Backup & Replication today! To learn more visit our website.

Share this report with your peers