Enabling Rapid and Effective IT Recovery

DR insights and tips for small and mid-sized businesses

Dale Vile and Tony Lock, Freeform Dynamics Ltd, October 2011

IT vendors and analysts sometimes make statements about SMBs not 'getting' the importance of disaster recovery (DR). But how true is this? And for those taking measures to allow recovery of IT systems and data in the event of a major incident or disaster, how well are they doing and what are their options for improvement?

Key Points

Most SMBs take measures to permit systems recovery following a major operational incident

Despite the focus of suppliers and advisors on large enterprise when it comes to DR, the results of a recent study based on feedback from 160 SMBs across the UK, France and Germany confirm that DR is important for all sizes of organisation. Furthermore, most SMBs put DR measures in place, albeit with varying degrees of formality and completeness.

However, significant gaps and shortfalls often exist

While efforts are clearly being made, when we look at specific DR capability to do with the IT and information related aspects of business operations, some clear gaps and shortfalls are highlighted. These are associated with a range of issues from the completeness and reliability of protection, through the speed and granularity of recovery, to the ability to test and operate cost-effectively.

DR initiatives often fail to compete effectively for attention, time and funding

The harsh reality for those interested in driving improvement is that DR initiatives are competing for priority with other projects that will often deliver more obvious value in terms of new or improved functionality for business users. In comparison, the value of DR related investments often only becomes clear when things go wrong.

The trick is to take a fresh view, bearing in mind the broader dynamics

As IT is relied on more extensively within the business, the potential risk clearly escalates, but so too do the cost and overhead of managing DR effectively through incremental manual approaches. Using a combination of thoughtful leverage of IT related developments in areas such as distributed operations and virtualisation, however, a lot can be achieved with minimal additional investment that can reduce both cost and risk.

Costs and risks can be further reduced through more advanced automation solutions

Many techniques and solutions that can enhance the level of protection and automation but have hitherto been the preserve of large enterprises are now more accessible to SMBs. Some of these are sold as discrete product offerings by vendors, with 'SMB friendly' packaging and pricing, but it's increasingly common to see advanced DR functionality embedded in storage systems, systems management tools, and so on.

Focusing on key enablers will enhance the returns from any DR improvement initiative

The research highlights 7 key enablers of effective IT DR, which are outlined in this report and should not be beyond the reach of any SMB IT department. It is therefore recommended that those looking to drive improvements take note of what has worked for others and learn from their peers.

This report is based on a research study designed, conducted and interpreted by Freeform Dynamics Ltd. 160 respondents from small and medium businesses across the United Kingdom, France and Germany were interviewed. The research was sponsored by Quest Software and completed during the first quarter of 2011.

Contents

Introduction 3
A note on study design 3
Checkpoint on current status 4
Taking a fresh view 5
7 enablers of effective IT DR 6
Pulling it all together 9

Appendix A: Profile of respondents and their environment 10
Appendix B: Assessing current IT DR capability 12
Appendix C: Evolution of traditional file-based backup practices 13
Appendix D: IT DR tools and techniques 14

About Freeform Dynamics… 16
About Quest Software 16
Terms of Use 16

Introduction

IT systems and the information they contain have become very important, often critical, to organisations of all sizes. Protecting the business from the consequences of IT failure or data loss is therefore a fundamental part of managing risk. So too is getting systems and information back online following some other kind of disaster such as a fire, flood or another unexpected event that affects business premises and facilities.

In response to this, larger enterprises tend to put formal plans in place for what is commonly referred to as 'Disaster Recovery' (DR), and IT vendors target them with a range of solutions designed to help with the protection and recovery process. Consultants and others offering DR related services have similarly been focused on the higher end of the market, educating large organisations for decades on both the issues and how to deal with them through a combination of best practice and technology.

Until quite recently, small and mid-sized businesses have been underserved in this whole area. The price tags and sophisticated nature of more advanced solutions have traditionally made them inaccessible to those working in a smaller scale environment where the IT function is often constrained in terms of bandwidth and specialist skills. But all this is changing very rapidly. Many suppliers are now making the effort to package and price solutions for smaller businesses, and either directly or indirectly via partners, ensuring that advice and guidance are more widely available.

With this in mind, Freeform Dynamics executed a study during the first half of 2011 to investigate how small and mid-sized organisations (with 50 to 250, and 250 to 1000 employees respectively) deal with IT related operational risk. One aim was to provide insights into current practices, issues and challenges that would help those responsible for this area to assess their performance with reference to input from their peers. A second, equally important, objective was to analyse what has the greatest impact on levels of protection, and derive a set of high level pointers to best practice for those looking to improve their approach.

The results of this study, which are based on feedback gathered during interviews with 160 small and mid-sized businesses (SMBs) across the UK, France and Germany (see Appendix A for details of demographics and nature/scale of IT infrastructure) are summarised and discussed in this report.

A note on study design

When designing research it is important to ensure that the terminology used during interviews is unambiguous and properly understood by participants. Preliminary work for this study suggested that particular attention needed to be paid to this when investigating DR, as a lot of the jargon in the area is only really meaningful to suppliers and specialists working in a large enterprise context.

Taking this on board, we started out the DR discussion with each respondent by presenting a very straightforward description of what we wanted to cover as follows:

> *"No matter how well we manage our business and IT environment, from time to time, things go wrong, often beyond our control, that have major consequences from an operational perspective. The kinds of things we are thinking of here are fire, flood or failure of a critical component in your IT system, as well as criminal damage or simply the mistakes humans sometimes make that have catastrophic consequences."*

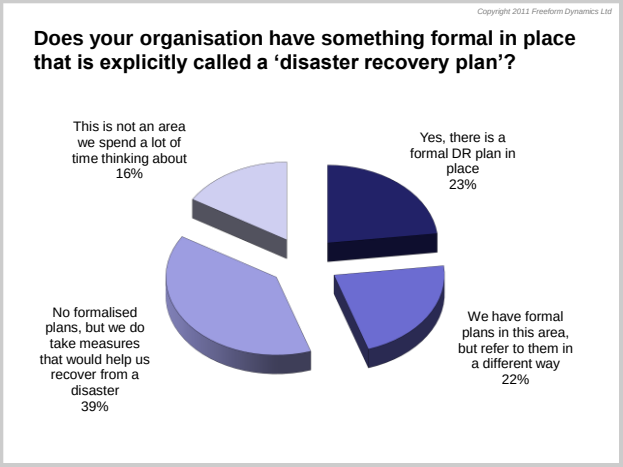
Interviewers then clarified as necessary to make sure that respondents were comfortable with the conversation we were seeking. It was then agreed that the term 'disaster recovery', or 'DR' for short, would be used to refer to the area described from that point onwards in each interview.

As interviews progressed, we also took care to check respondent familiarity with some of the more specific terminology around solutions and techniques commonly used in DR circles, and define terms in simple language where necessary. We'll make reference to these definitions as we go through this report.

In the meantime, let's start our discussion by looking at the degree to which those responsible for IT in an SMB environment appreciate and care about DR.

Checkpoint on current status

It is not uncommon to hear IT vendors and analysts make statements about SMBs not 'getting' the importance of DR. The results of our study, however, confirm that a large majority of SMBs do put DR measures in place, albeit with different degrees of formality, and often describing plans and activities using different language (Figure 1).



SMBs care about DR, but employ different degrees of formality when dealing with it, and use different language to describe what they are doing.

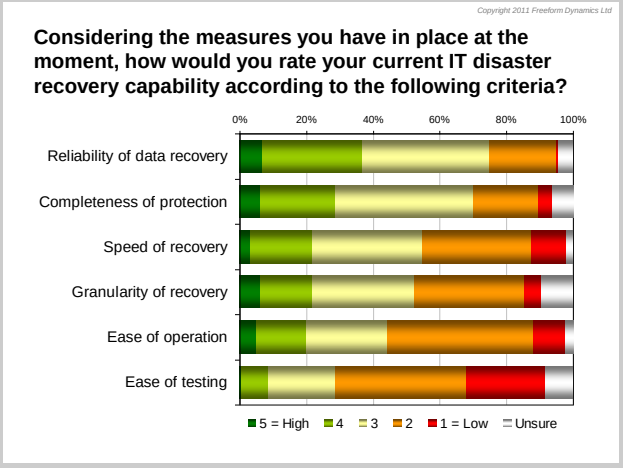
Figure 1

Picking up on the question of terminology, while we haven't shown it explicitly here, we do see clear evidence of a language gap. Fewer than two in five believe that others in their organisation would know what was meant by the term 'DR', for example, with a similar number saying their colleagues would only have a rough idea of its meaning.

The danger is that those working in an SMB environment assume that DR is all about grand plans, the kind which revolves around redundant data centres and empty offices with rows of vacant desks sitting there waiting to accommodate a workforce made homeless by a fire or flood.

Unfortunately, it is all too easy to miss the conversations that take place under the DR umbrella which simply relate to making IT systems more resilient and recoverable.

This 'IT DR' topic is relevant to businesses of all sizes. Furthermore, the research points to a real need. Despite most SMBs taking proactive DR measures, when we look at specific capability to do with IT and information related issues, some clear gaps and shortfalls are highlighted (Figure 2).

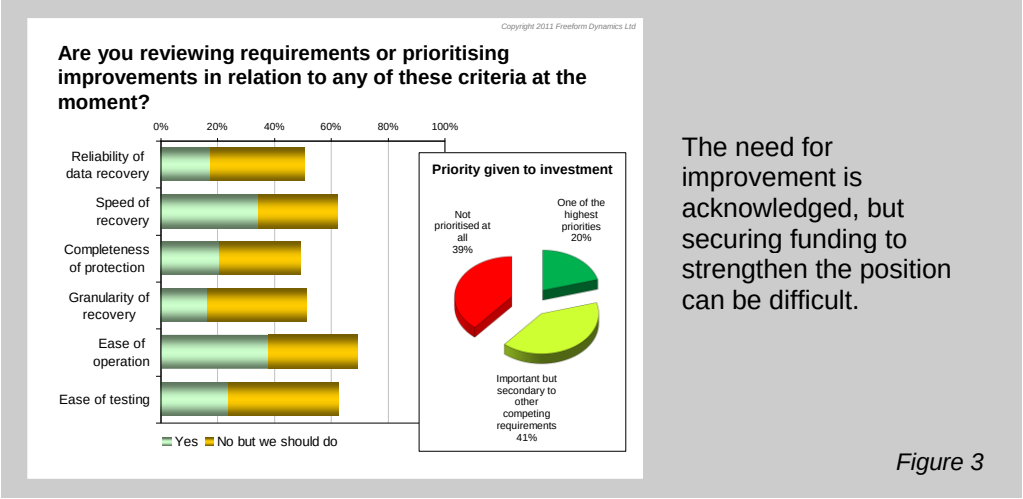


Capability gaps and shortfalls are common.

(See Appendix B for more complete definitions of the capability areas listed on this chart)

Figure 2

Not surprisingly, many acknowledge the need for improvement, but indications are that securing funding to improve things can be a challenge (Figure 3).



The need for improvement is acknowledged, but securing funding to strengthen the position can be difficult.

Figure 3

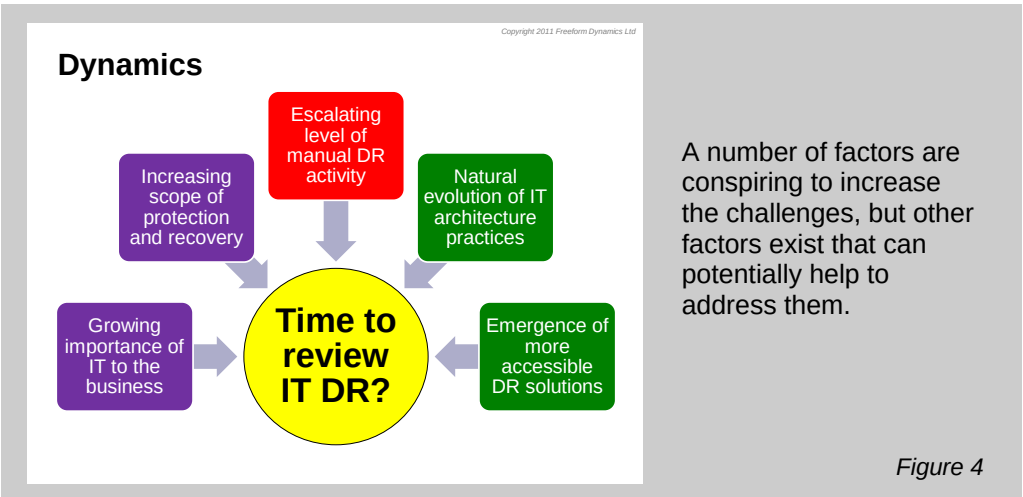
The reality is that DR improvement initiatives are competing for attention and funding with other projects that will often deliver more obvious value in terms of new or improved functionality for business users. In comparison, the benefit of DR related investments only becomes clear when things go wrong. The harsh reality is that unless there has been a recent incident that has impacted the business significantly, the value of any risk management initiative is often underappreciated.

Taking a fresh view

A common problem with business risk in general is a tendency for organisations to make a point-in-time assessment, put appropriate measures in place, and then essentially forget about them. The upshot is that measures do not consciously get reviewed that often.

This is particularly relevant when considering IT DR because the ever growing importance of IT to the business clearly brings with it a corresponding level of potentially escalating risk. Meanwhile, as a result of IT infrastructure and information needs within even quite small organisations becoming increasingly broader and more complex, the scope of protection and recovery activity continues to grow. The time and effort spent on IT DR then creeps up, often with no one really noticing, leading to a lot of inefficient manual activity, with the cost and overhead that comes with that.

Fortunately, the natural evolution of IT architecture and practices, particularly in areas such as distributed operations and virtualisation, opens up opportunities for more cost effective IT DR approaches. This is further helped by the emergence of more accessible and affordable DR solutions that can enable better automation as well as increasing the level of protection (Figure 4).



A number of factors are conspiring to increase the challenges, but other factors exist that can potentially help to address them.

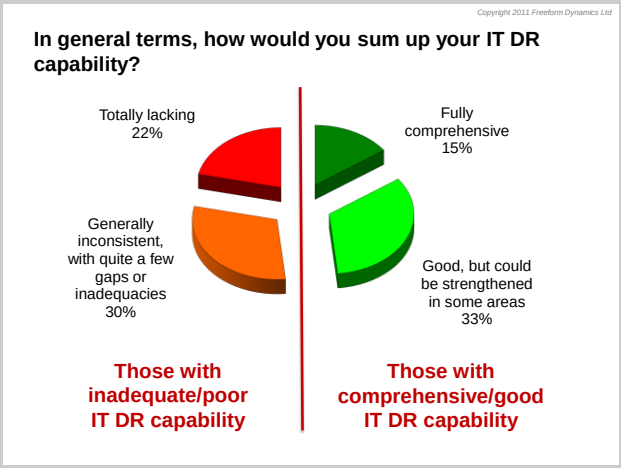
Figure 4

The point of all this is that effective IT DR nowadays is not about throwing money at the problem. A lot can be achieved by thoughtfully exploiting natural changes that are likely to be occurring

anyway. And where additional investment does make sense, this will often pay back in the form of reduced IT overhead and cost.

So much for the theory, but is any of this backed up by the research?

We can investigate this by dividing our research sample into two groups based on how they sum up their overall IT DR capability (Figure 5):



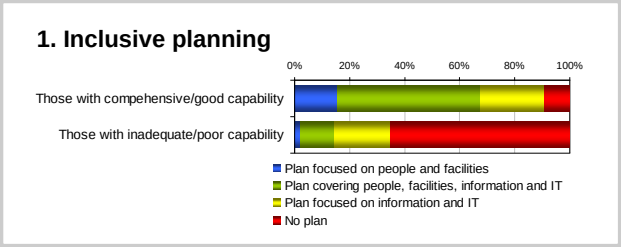
For analysis purposes, the sample can be divided into two roughly equal groups based on performance.

Figure 5

Comparing the two groups, we observe some significant differences between them, with seven specific characteristics or behaviours standing out as enablers of better performance.

Seven enablers of effective IT DR

Firstly, those reporting more comprehensive/good IT DR capability are over twice as likely to have explicit DR related plans in place, and those plans are more likely to be inclusive, considering information and IT related risks alongside risks relating to people and facilities (Figure 6).

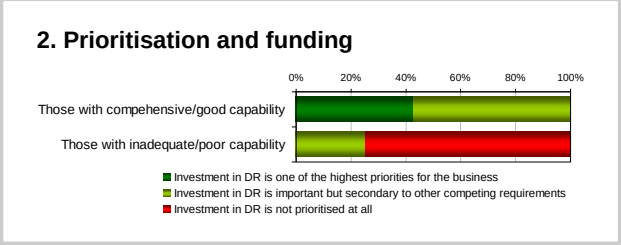


DR touches many aspects of the business, so inclusive plans taking dependencies into account are important.

Figure 6

This makes sense as the planning process itself tends to make people think more about the kinds of events that could disrupt IT or business operations. Taking an inclusive approach then makes sure that dependencies between business and IT operations are fully appreciated when looking at risk scenarios and recovery options.

Of course assessment and planning is only of any use if action is taken as a result, and this in turn is dependent on the allocation of time, attention and, where necessary, funding (Figure 7).



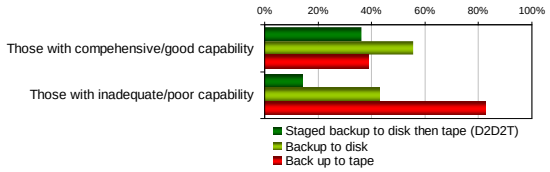
Good IT DR does not happen without explicit commitment. Better performers prioritise resources and funding.

Figure 7

Even if funding is tight and the ability to make capital investments on equipment and tools is limited, as we said earlier a lot can be achieved by simply adopting a different approach.

One example of this is in relation to traditional file-based backup and recovery, which is clearly a fundamental part of IT DR, but has traditionally revolved around the use of magnetic tape. The evidence tells us, however, that while tape remains important, making more use of disk-based storage as a backup medium is associated with better IT DR performance (Figure 8).

3. Emphasis on disk rather than tape



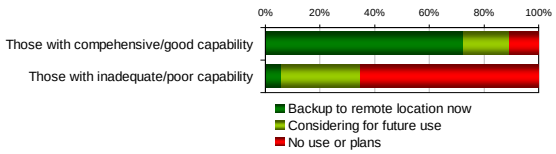
Using disk rather than tape as a primary backup medium can improve the speed and granularity of the recovery process.

Figure 8

The benefit of disk as a primary backup medium from a recovery perspective is that it better enables rapid and selective retrieval of information, with obvious advantages in terms of recovery.

Apart from the media used as a target for backups, another consideration is the location of the backup device. From a DR perspective, backing up locally is OK if media is then transported off-site for safe keeping quickly afterwards (see Appendix C for current practice here), but backing up across a network, bandwidth and speed permitting, means data is protected from a local catastrophe such as a fire or flood almost immediately. Those that are more confident in their DR capability tend to use this technique much more than others (Figure 9).

4. Use of remote facilities

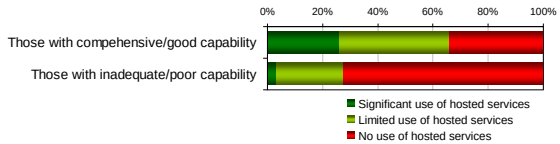


Sending backups or second copies of data directly to a remote device reduces exposure to local issues.

Figure 9

The problem when considering remote backup, however, is that many organisations do not have a second site under their control that can be used for this purpose (see Appendix A for physical distribution of operations), which brings us to the use of service provider resources (Figure 10).

5. Use of hosted services



Hosted services can help with remote backup and access to providers' DR facilities. Recovery to the cloud is also possible.

Figure 10

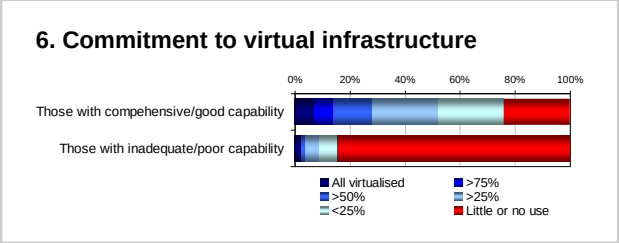
Anecdotal feedback from respondents tells us that infrastructure hosting, which is now readily available at reasonable cost to SMBs, assists with DR in three main ways.

Firstly, hosted storage can be used as a target for backups and/or the maintenance of second copies of live data for those without a second site of their own. Secondly, where hosted servers and storage are used for live operations, the organisation can benefit from the DR facilities put in place internally by the service provider. Any reputable provider, for example, will be able to deal with backup and recovery within their own data centre environment in way that most SMBs would find

difficult to match. Furthermore, a provider will often be able to offer enhanced resilience (through redundant infrastructure) and/or rapid/immediate fail-over in the event of a problem occurring with servers they are hosting on your behalf.

The third way in which hosted infrastructure can be used is to facilitate remote recovery. Should the local server room get flooded or even a single critical server fail catastrophically, the applications and data can be restarted in the hosted environment. Some people nowadays are using phrases such as 'failover to the cloud' or 'recovery to the cloud' to describe this principle.

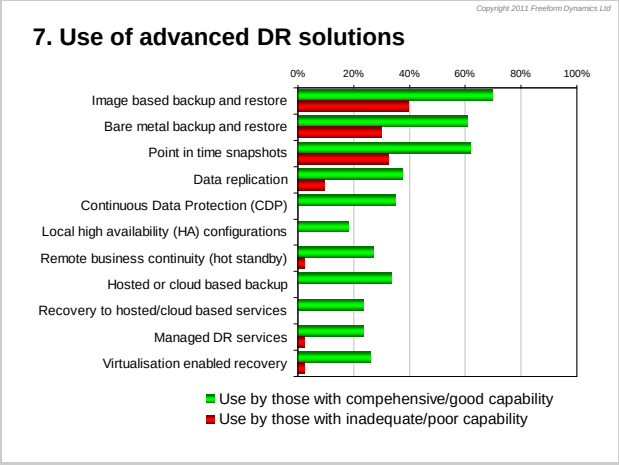
This kind of approach, and indeed rapid recovery and recovery testing in general, is made easier with the advent of virtualisation. Efforts made to virtualise server infrastructure for consolidation and cost saving purposes (see Appendix A) can therefore be leveraged to improve DR (Figure 11).



Spinning up virtual images on alternative local, remote or hosted servers enhances speed and flexibility of recovery.

Figure 11

The last of the key enablers we shall mention is a bit of a catch-all. Organisations claiming superior DR capability are more likely to have adopted one or more of the advanced solutions and approaches that have hitherto been the preserve of large enterprises (Figure 12).



Modern DR technology and techniques can cut out manual processing and allow approaches to be implemented that improve the speed, comprehensiveness, granularity and reliability of IT DR processes.

Figure 12

Many of the techniques we see here are aimed at improving the responsiveness and granularity of the protection and recovery process by moving from a periodic backup to a snapshot approach or a more continuous protection scheme.

Second copies of live data that are kept up-to-date on a near real-time basis through data replication, for example, can be switched to as soon as the application is up and running again following a failure – almost immediately in the case of hot standby. Techniques such as CDP that keep a continuous log of changes to information can allow rollback or recovery to a specific point in time in the event of an application or user error corrupting a data store by sending incorrect data to it, accidentally deleting something important, or otherwise invalidating the 'current state'.

It is beyond the scope of this report to go into detail on all of the techniques and solutions available, but a brief description of each (that was used during research interviews) is provided in Appendix D. Suffice it to say that if you have never explored this area in-depth before or haven't done so in a while, then you might be surprised at some of the options available if you do some research. You will also find that the abovementioned advanced capabilities are sometimes available as options, or even as embedded functionality, within storage systems, management tools and so on.

Pulling it all together

Organisations vary in terms of their exposure and attitude to risk, and this obviously has an impact on the kind of IT DR that is appropriate. However, things are constantly changing in both the technology industry and the way IT and information is used within the business, so periodically reviewing IT DR measures is important from both a risk and cost management perspective.

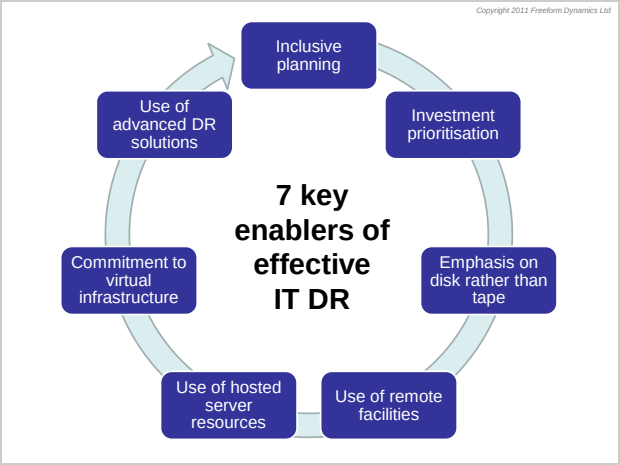
When conducting reviews, we would recommend an objective business-led approach, focusing on some of the key parameters we have touched on in this report:

- Scope of required protection and recovery
- Completeness of protection coverage
- Reliability of recovery measures and processes
- Speed and granularity of recovery processes

We know from our study that many acknowledge gaps and shortfalls in some or all of these areas at an overall capability level. When evaluating or reviewing requirements, however, it makes sense to be more specific, and look at each parameter in relation to individual scenarios, systems and information stores. This is because some systems and information may be more critical than others, so it might not make sense to apply the same level of protection across the board.

When looking at how to deal with requirements, we must also remember that risk management in any context is all about probability, so it's less about absolutes and more about stacking the odds in your favour.

With this in mind, it's noteworthy that when we looked at those achieving better performance with IT DR, we didn't find one magic bullet for success, but a range of factors that each contribute to creating a safer and more resilient business and systems environment (Figure 13).



While no single magic bullet exists, a number of enablers have been identified that are likely to improve IT DR capability.

Figure 13

When we were analysing the data and we ended up with this set of correlations, we were tempted to refer to "The 7 enablers of effective IT DR" as a hat-tip to Stephen Covey and his book "The Seven Habits of Highly Effective People". We dropped the 'The', however, in acknowledgement of the fact that ours is almost certainly not *the* definitive list, and the last item we call out, to do with more advanced DR solutions, is a bit of a catch-all anyway.

On that note, the other big finding from the study is that those operating in a small or mid-sized business environment generally need to get more up to speed with solutions beyond traditional file-based backup and recovery. Just like many other areas of IT, developments in DR have led to a reduction in both cost and complexity, and a lot of the technologies and techniques that were the preserve of the large enterprise a few years ago, are now much more accessible to SMBs.

The bottom line message to those responsible for the IT aspects of risk management in a smaller business environment is therefore to do a bit of research and get up to speed with what's available. We hope this report has helped to get you off on the right foot.

Appendix A: Profile of respondents and their environment

The study upon with this report is based was designed, conducted and interpreted by Freeform Dynamics Ltd and completed in the first quarter of 2011 with sponsorship from Quest Software.

A cross section of Western European SMBs were interviewed (Figure 14) with varying scales of IT system in place (Figure 15) and degrees of operational distribution (Figure 16).

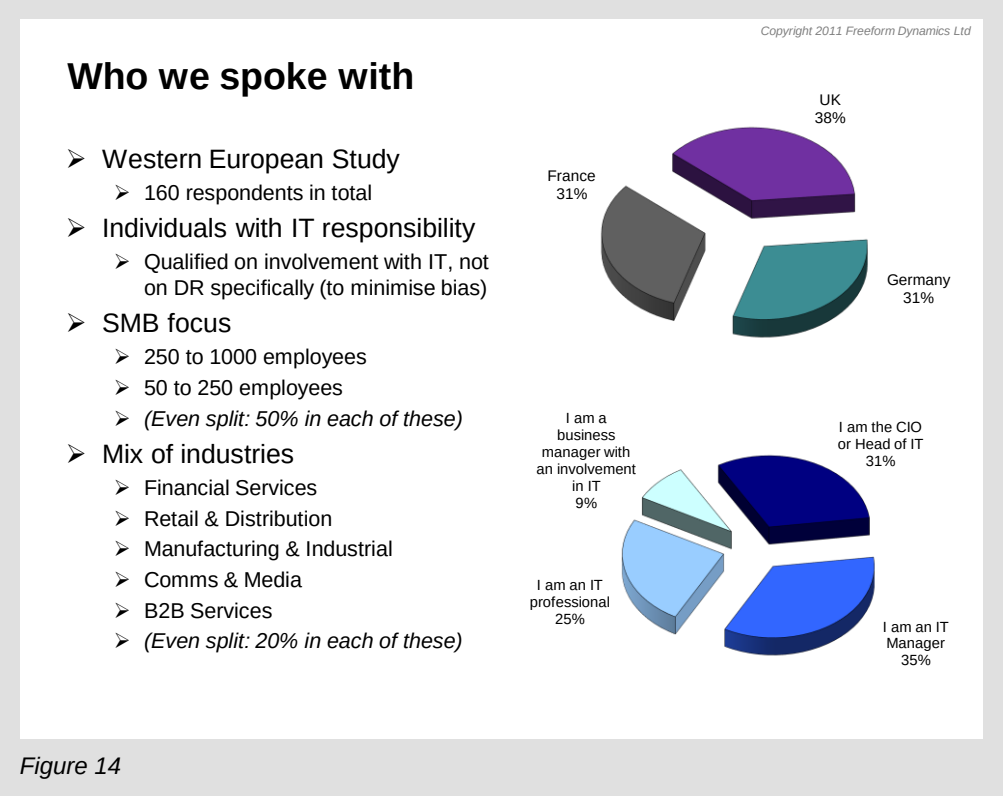


Figure 14

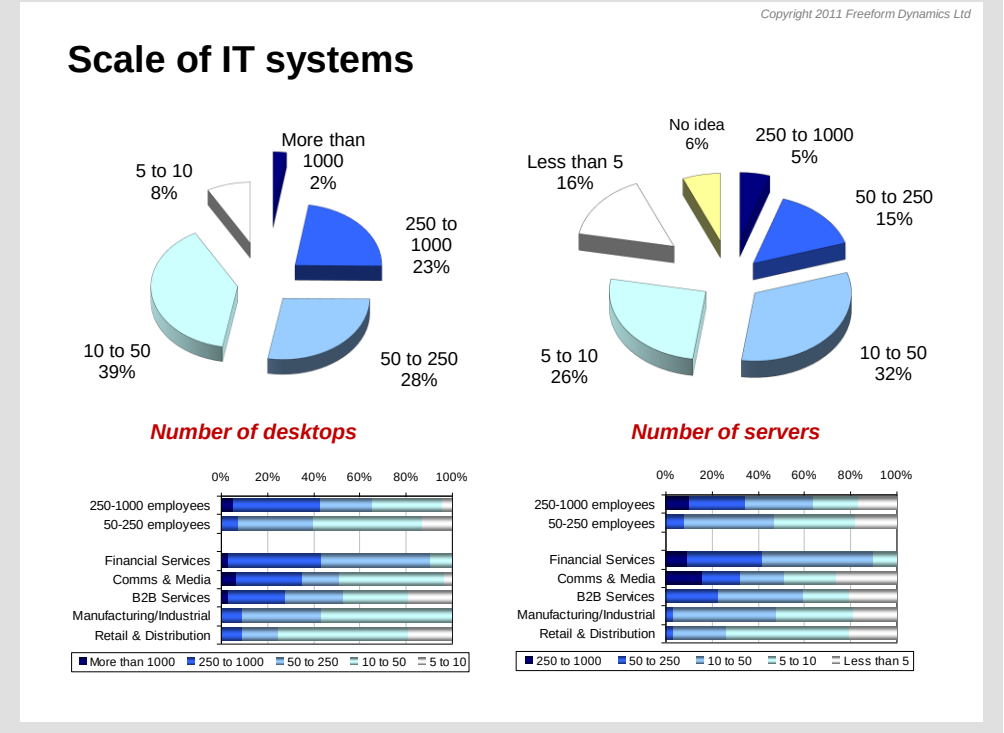


Figure 15

Physical distribution of operations

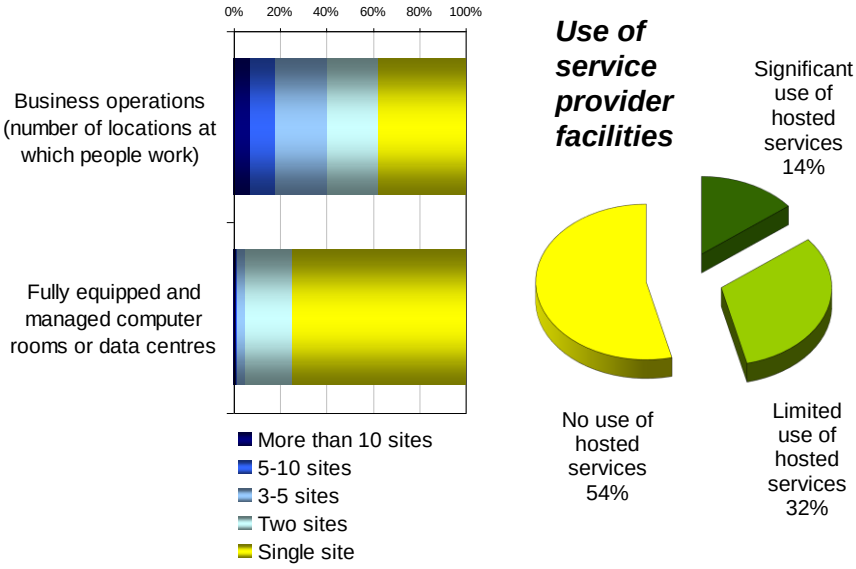


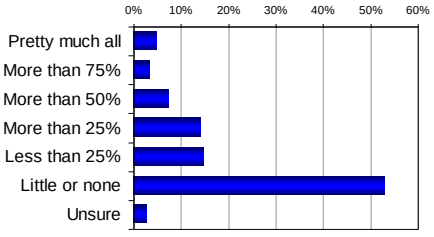
Figure 16

As discussed in the body of this report, related to the use of hosted services shown above is the nature of the server environment and the degree to which it has been virtualised (Figure 17).

The server infrastructure in more detail

- x86 infrastructure predominates
- The majority of servers run Windows
- But it's still early days for virtualisation

What proportion of your overall x86 server infrastructure would you estimate to be virtualised at the moment?



Do you see this increasing over the coming three years?

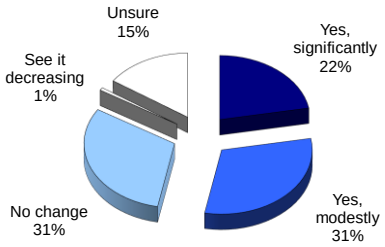


Figure 17

Appendix B: Assessing current IT DR capability

A number of parameters relating to the effectiveness of IT DR measures were investigated during the study. A more expanded description of each is provided in Table 1:

Table 1: Parameters for assessment of IT DR capability	
Reliability of data recovery	The ability to meet business expectations in terms of recovery from a disaster with minimal loss of protected data.
Completeness of protection	The ability to backup and recover all of the business information and system configuration data you ideally need to.
Speed of recovery	The ability to meet business expectations for getting systems back up and running quickly to minimise disruption.
Granularity of recovery	The selective ability to roll back to a specific point in time or recover a previous version of an object following loss or corruption.
Ease of operation	Minimisation of the cost and overhead of protecting and recovering data and systems from an IT budget and resource perspective.
Ease of testing	The ability to regularly check that protection and recovery mechanisms are actually doing what they are supposed to.

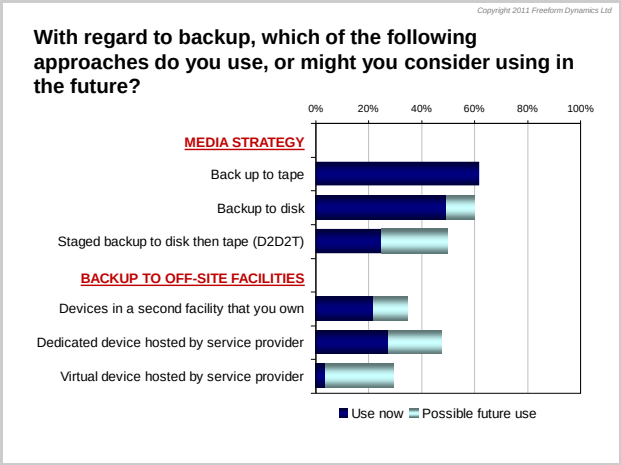
Just looking at this list is useful in its own right. Consultants and other advisors in the DR space view the world routinely in this way. Many of the people interviewed in our study, however, were not used to considering risk and recovery in such precise terms.

Whether you adopt the language shown here is immaterial, but considering capabilities clearly in the manner we have listed when IT and business management are reviewing requirements often helps to focus the mind on real needs in a precise and unambiguous way.

Appendix C: Evolution of traditional file-based backup practices

The mostly frequently used approach for dealing with IT DR needs today is file-based backup. While more advanced solutions are becoming relevant in this space, the study did reveal some evolution taking place around the way traditional backup is implemented.

Firstly, we see a shift in emphasis of the primary backup medium from tape to disk, with a general trend towards staged 'disk-to-disk-to-tape' (D2D2T) methods (Figure 18).

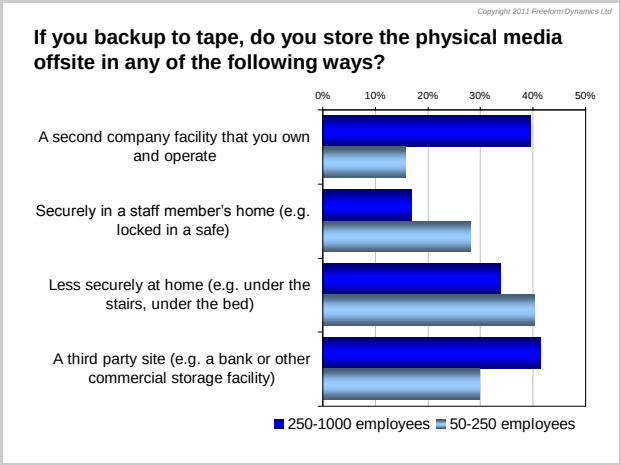


We see more emphasis on disk, with a trend towards staged backup. Direct backup to remote facilities of various kinds is also starting to be used by some, though network constraints can limit adoption here.

Figure 18

We can also see from this chart that direct backup to off-site facilities is beginning to happen, and we expect more of a trend in this direction as the use of cloud and hosted services in general continues to mature.

In the interim, we picked up a great deal of variability in terms of how backup tapes, once produced, are handled (Figure 19).



Some SMBs are very careful about what they do with their backup tapes, but others could possibly be exposed.

Figure 19

What's surprising here is the number of even mid-sized organisations that store backup tapes in relatively insecure places in staff members' homes, which could represent a higher risk of damage and corruption, and if encryption is not used, exposure in terms of security and/or compliance.

The challenge is that many backup and recovery processes are put into place then forgotten, and never revisited as the organisation grows and/or IT systems evolve and become more sophisticated and business critical.

As file-based backup and recovery is likely to remain part of any IT DR plan, a must for any SMBs that have not done so recently is to review their procedures in this area.

Appendix D: IT DR tools and techniques

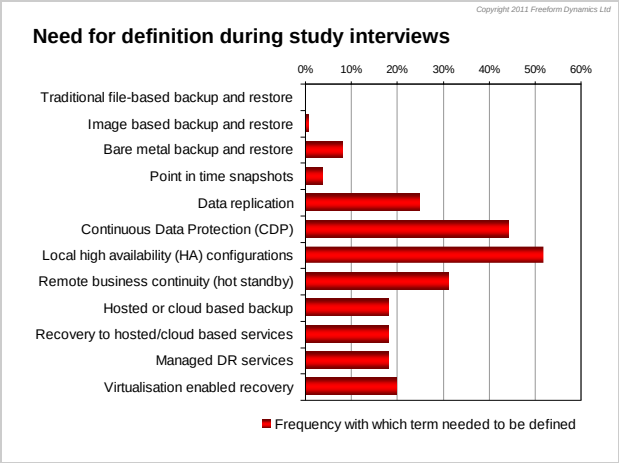
Some IT DR solutions are sold as discrete product offerings by vendors, but it's becoming increasingly common for advanced DR functionality to be embedded as 'features' in storage systems, systems management tools, and so on.

The range of techniques investigated in our study can be seen in Table 2 below:

Table 2: Solutions and definitions	
Traditional file-based backup and restore	Backup of file system contents to tape or disk. Includes both complete and incremental backups, and the backup itself may or may not be compressed or encrypted, depending on the tools that are used.
Image based backup and restore	A block–by-block copy of the disk is made, allowing that disk to be recovered exactly as it was backed up. Modern systems maintain meta-data with the backed up image to allow selective recovery, e.g. the retrieval of a single file, without having to reload the entire image.
Bare metal backup and restore	Backup of a complete server, including system and application software as well as data, in a form that can be reloaded onto an alternative physical machine as part of the recovery process. The new machine typically needs to be similar but not identical to the original.
Point in time snapshots	As the name suggests, this technique is based on taking periodic snapshots of the information being protected. Similar in principle to traditional backup, but often used to create remote copies of data across a network that are then available quickly for recovery purposes.
Data replication	A technique used to create and keep a remote replica of data up to date on a continuous basis through continuous synchronisation as changes occur. Often used as part of a 'hot standby' solution (see below).
Continuous Data Protection (CDP)	A mechanism for providing ongoing protection. Works by keeping a separate record or log of all changes made to a data store so it can be rolled back or recovered to a specific point in time in the event of a failure or corruption.
Local high availability (HA) configurations	Hardware or systems software based mirroring of tightly coupled systems or clusters allowing rapid failover in the event of a component failure. The basic idea is to prevent systems originating disasters occurring in the first place.
Remote business continuity (hot standby)	The concept of maintaining a second system on a remote site in a state that allows direct fail-over in the event of a disaster. Unlike local HA, the business is protected against disasters affecting a complete site (e.g. fire, flood, power failure, etc).
Hosted or cloud based backup	Use of physical or virtual storage facilities in a service provider environment for remote backup purposes.
Recovery to hosted/cloud based services	The notion of using hosted resources for recovery purposes, e.g. provisioning cloud based servers and storage in the event of a failure that can be used in place of on-premise equipment that has become unavailable. You get up and running by loading your backups into the cloud.
Managed DR services	Specialist services delivered by a third party to implement disaster recovery measures. Can be based on any combination of the mechanisms we have been discussing.
Virtualisation enabled recovery	The technique of recovering from backup onto virtual servers to minimise the need for standby or replacement hardware. This technique also potentially has benefits in terms of recovery testing.

The definitions we have provided are based on our frequent conversations as industry analysts with IT vendors. These are the same as the terminology and descriptions we see included in sales and marketing literature, sales presentations and analyst reports that are typically aimed at larger enterprises.

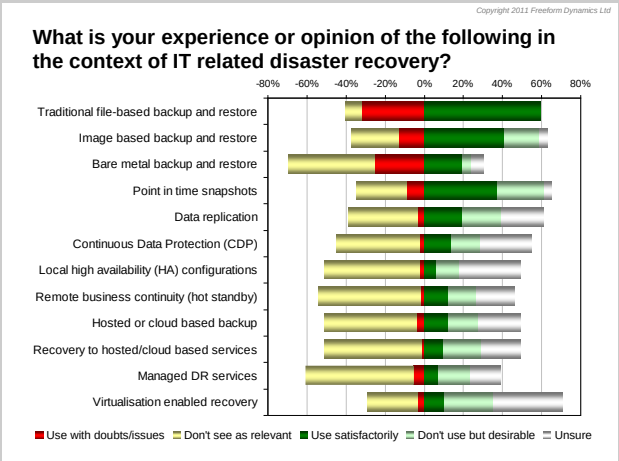
On the premise of not assuming prior familiarity with the jargon, we ran through the above list and asked respondents if they needed a definition of each term during interviews, and in many cases it was clear that they did (Figure 20).



Many non-specialists working in an SMB environment are unfamiliar with the technology and techniques discussed when vendors engage with large enterprises.

Figure 20

Turning to what's actually being used by SMBs, the emphasis is currently on traditional file-based backup and recovery, with an apparently good level of adoption of image based techniques and point-in-time snapshots (Figure 21).



The emphasis is currently on traditional file-based backup and recovery, with some use of image based techniques and snapshots, though the latter are likely to be managed manually. Experiences with more advanced solutions are generally positive.

Figure 21

Having discussed these results with a few specialist vendors, it is worth noting that some of the activity shown could be a bit misleading. When IT professionals in the SMB space talk about image based backup and point-in-time snapshots, they are generally referring to taking periodic manual 'dumps' of disks or file systems. Vendors, on the other hand, use the same terms to refer to specific tools that automate or streamline the process, and allow full monitoring and control of activity, along with more selective recovery, to work around the 'all or nothing' recovery constraint in this area.

The vendors we have spoken with tell us that uptake of such solutions in SMBs is actually still quite limited, and the same can obviously be said for other more advanced solutions as we can see. However, we can also see that experiences have generally been positive, confirming that more advanced solutions can be used successfully in a smaller business and IT environment.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.

About Quest Software

Quest Software (Nasdaq: QSFT) simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments.

For more information about Quest solutions for application management, database management, Windows management, virtualization management, and IT management, go to www.quest.com.

Terms of Use