

**The
Symantec
Disaster
Recovery
Research
2007**

**Independent Market
Research Report**

Commissioned by



October 2007

Copyright notice

The copyright of this independent market research report remains with Dynamic Markets Limited, regardless of the medium this report may be stored in. The report may be reproduced, but only in its entirety; no abridgements or additions may be made without the specific written consent of Dynamic Markets Limited.

Report Author:

*Dr Cherry Taylor BSc PhD
Dynamic Markets Limited
PO Box 19
Abergavenny
NP7 8YF
UK*

Table of Contents

1. Summary.....	1
2. Research Methodology.....	9
3. Key Findings.....	13
3.1 Triggers for creation of DR strategy and plan.....	13
3.2 Business continuity plan in relation to DR plan.....	19
3.3 Location of DR plan	22
3.4 Storage media for DR plan	28
3.5 Composition of DR committee.....	31
3.6 Investment in DR plan in hard economic times	37
3.7 Technology covered by DR plan	40
3.8 Frequency of testing DR plan.....	47
3.9 Reasons for failure of DR plan tests.....	53
3.10 Barriers to testing DR plan	56
3.11 Agreeing acceptable levels for risks.....	61
3.12 Percentage of business-critical applications.....	64
3.13 Poor application performance and the DR plan	69
3.14 Main threats or disasters exposed to without DR plan.....	72
3.15 Threats that have been assessed.....	77
3.16 Top 5 consequences of a disaster	81
3.17 Execution of the DR plan for real.....	85
3.18 Time needed to recover after a fire disaster	90
3.19 DR plans of suppliers.....	102
3.20 Importance of Internet presence	105
3.21 Reasons for not having a DR plan	108
3.22 Threats and disasters experienced by those without a DR plan..	112
Appendix A: Quantitative Questionnaire	115

1. Summary

The rising profile of DR?

The makeup of the DR committee? [Section 3.5]

- This research shows very clearly that the makeup of the decision making unit for DR has changed considerably in the last 3 to 4 years.
- There has been an elevation of the issue to higher levels within the organisation, and there has been an influx of non-IT roles in to the decision-making process.
 - Today, more (23%) involve the CEO, compared to 2003 (7%) and 2004 (8%).
 - More (17%) involve other directors, compared to 2003 (11%).
 - More (17%) include a chief security officer, compared to 2003 (4%) and 2004 (9%).
 - More (55%) involve the CIO / CTO / IT director, compared to 2003 (22%) and 2004 (36%).
 - More (34%) include systems / infrastructure managers, compared to 2003 (8%) and 2004 (9%).
- But still only 43% of organisations give DR committee membership to a mix of IT and non-IT staff – but this is a dramatic improvement from 11% in 2003 and 25% in 2004.
- However, 1 in 2 organisations (49%) still only involve IT staff on the DR committee – but this situations is a significant improvement on 2003 (75%) and 2004 (64%).
- Regionally, more EMEA organisations seem to take this mixed roles approach, compared to their US counterparts:
 - EMEA organisations involve a wider variety of roles, compared to the US.
 - More (56%) include the CIO / CTO / IT director, compared to the US (42%).
 - More (12%) include the line of business heads, compared to the US (5%).
 - More (18%) include other directors, compared to the US (9%).

Fearred consequences of a disaster? [Section 3.16]

- The influx of non-IT personnel may be due to the fact that at the top of the list of concerns over potential disasters is damage to brand reputation (69%).
- This is followed by 65% who fear damage to customer loyalty and the same amount fear damage to their competitive standing in the market place.
- Almost as many (64%) are concerned about data loss as a potential impact or consequence of a disaster.
- EMEA organisations are especially worried about decreased employee productivity and a reduction in revenue, compared to US organisations.
- Whereas US organisations are especially concerned about damage to brand reputation and to supplier relationships, relative to EMEA.

Investment in DR? [Section 3.16]

- This change in profile of the DR decision making team is very likely to affect decisions on DR funding.
- Indeed, for the largest group of organisations (40%), all ongoing investment in DR would be maintained and safeguarded if their organisation were to fall on hard economic times tomorrow – and this is more than in 2004.
- Another 34% say investment would be reduced, but it would still carry on.
- But only 3% of organisations say investment would be increased in hard economic times, if deemed necessary.
- In contrast, 19% of IT managers say the investment in DR would be frozen and all activity would be put on hold if such circumstances were to arise – a sentiment that is especially common in the US (28%), compared to EMEA (18%).

Prompts for creating the DR plan? [Section 3.1]

- The Top 3 issues that have prompted organisations to create a DR plan and strategy are:
 1. Natural disasters (69%)
 2. Virus attacks (57%)
 3. War and / or terrorism (31%)
- Overall, US organisations were prompted by more factors, compared to EMEA organisations - in fact, more US organisations were prompted by war and / or terrorism, virus attacks and increased number of people working from home, compared to EMEA organisations.
- But, more EMEA organisations were prompted by Government and industry sector regulations and changes in technology infrastructure compared to US organisations.
- Since 2004, the amount of organisations that have been prompted to create a DR plan and strategy by natural disasters, war and / or terrorism, virus attacks and by accidental or malicious employee behaviour has increased.
- Less significant in 2007 are insurance policies, pressure from customers, suppliers and their competition, increases in patches and changes in technology.

Levels of risk? [Sections 3.11 and 3.14]

- The Top 3 threats or disasters that organisations would now feel exposed to if they did not have their DR plan in place are:
 1. Natural disasters, e.g. fire and flood (70%)
 2. Computer failure, i.e. hardware and software (67%)
 3. External computer threats, e.g. viruses and hackers (57%)
- US organisations would feel exposed to more threats without their DR plans than those in EMEA, and would be more worried about some specific ones, compared to EMEA:
 - More (55%) would feel exposed to man-made disasters, compared to EMEA (41%).
 - More (47%) would feel exposed to internal computer threats, compared to EMEA (34%).

- On the increase since 2003 and 2004, has been a concern about natural disasters, with more organisations questioned in 2007 (70%) saying they would feel exposed to this without their DR plan, compared to 2003 (59%) and 2004 (65%).
- But of less concern now in 2007, compared to 2004 and / or 2003, are man-made disasters, computer failure, external computer threats and internal computer threats.
- In total, 89% of IT managers have discussed and agreed acceptable levels of risk with the non-IT, business directors within their organisation for at least some of the threats they feel exposed to.
- But only a third (33%) have done so for all the threats they feel exposed to – 65% have not.
- Another 1 in 10 (9%) have not discussed nor agreed acceptable levels of risk for any threats.
- Also, more of those in South Africa and the Middle East have done this for all the threats they feel exposed to, compared to Russia.
- Interestingly, natural disasters, which is at the top of the list of threats that prompted organisations to first create their plan and is also the one that most would feel exposed to without their DR plan, does not make the Top 3 list of threats for which the levels of risk have been assessed and agreed.
- Natural disasters is actually the second most common trigger for execution of the DR plan, either in full or in part.

Probability and impact assessment? [Sections 3.15]

- While 88% of organisations have carried out a probability and impact assessment for at least 1 of the threats they feel exposed to, only 40% have carried these out for all the threats they feel exposed to, and 12% have not carried them out for any.
- However, the 3 most commonly assessed threats are:
 1. Computer system failure (73%)
 2. External computer threats (69%)
 3. IT problem management (67%)
- Once again, natural disasters, which is at the top of the list of threats that prompted organisations to first create their plan and is also the one that most would feel exposed to without their DR plan, does not make the Top 3 list of threats for which a probability and impact assessment has been carried out.
- The least assessed area is for configuration change management issues, where only 42% of people that feel exposed to this threat have carried out a probability and impact assessment.
- EMEA organisations have carried out such assessments for more of the threats they feel exposed to, compared to US organisations; and more US organisations (55%) have not carried them out for all the threats they feel exposed to, compared to EMEA (38%).

Comprehensive DR plans?

BC and the DR plan: [Section 3.2]

- There is often dispute among DR experts over the nature of the business continuity and disaster recovery plans and the degree to which they should be integrated.
- Among this research sample, opinion reflects this and is divided with 43% of organisations having a DR plan that is integrated with the BC plan, and almost as many (40%) having separate DR and BC plans.
- But, 10% have a DR plan only and no BC plan.
- However, this research indicates that there has been a move towards the integration of the two plans, with the amount of organisations with integrated DR and BC plan on the increase since 2004 (from 38% to 43%).
- But Russia stands out from the other countries by its lack of BC plans, whereas integrated BC and DR plans are most common in Poland.

What's covered by the DR plan? [Section 3.7]

- Most DR plans in 2007 cover database servers, applications, email and web servers, where they exist within an organisation.
- But fewer include the desktop environment, the laptop environment, remote offices, mobile technology and home workers' PCs.
- Indeed, the least included area is mobile technology, such as handheld devices.
- Interestingly, fewer organisations questioned in 2007 (87%) that have web servers in the organisation cover them in their DR plan, compared to 2004 (92%).

Application performance considered in DR plans? [Sections 3.12, 3.13 & 3.20]

- 94% of organisations consider at least some of their applications to be business-critical, and on average, 36% of an organisation's applications are given this status.
- But while opinion is quite varied, in general, more organisations (69%) cite a figure of 50% or below.
- While EMEA organisations generally consider more of their applications to be business-critical, compared to the US, those in Russia think very few are.
- Furthermore, 99% of organisations think their Internet presence is important to some degree or other to their overall business success – and 61% describe it as either critical (14%) or very important (47%).
- Yet despite the importance of applications to the success and smooth running of the organisation, only 30% say poor application performance would lead to them invoking their DR plan.
- In contrast, 62% say this would not be the case, and there is no difference in opinion between EMEA and the US on this matter.

- In fact, among those who think the Internet is either critical or very important to the success of their business, only 30% say poor application performance would lead to them invoking the DR plan – 64% say it would not.

Robustness of DR plans?

Testing the DR plan: [Sections 3.8-3.10]

- 91% of organisations carry out full scenario testing on their DR plans involving relevant people, processes and technologies – and on average this takes place once every 8 months.
- Indeed, just over half the sample (54%) test more frequently than annually and 34% carry out such tests annually or less frequently than this.
- Another 3% carry out full scenario tests on an ad-hoc basis and 8% do not carry out any full scenario testing.
- However, testing became more frequent between 2003 and 2004, and again it has seen another rise in the proportion of organisations testing every 6 months or less between 2004 and 2007.
- But the most frequent testing is carried out in Russia and the Middle East.
- However, 48% of organisations that carry out full scenario tests say these tests have failed, and the 3 main reasons are:
 1. The technology does not do what it is supposed to (22%)
 2. People do not do what they are supposed to (19%)
 3. DR processes turn out to be inappropriate (18%)
- Indeed, 21% say their tests have failed for more than 1 reason.
- These problems with testing apply equally to EMEA and the US.
- Despite the frequency of testing, 89% of organisations think there are barriers to carrying out full scenario tests on their DR plans, and the Top 3 barriers are:
 1. Resources, in terms of people's time (50%)
 2. Disruption to employees (47%)
 3. Resources, in terms of budget (38%)
- However, only 17% say other IT projects take a higher priority than full testing of the DR plan, and only 12% say it is not seen as a priority by top management.
- More US organisations think there are barriers, compared to EMEA:
 - More (62%) say disruption to employees is a barrier, compared to EMEA (46%).
 - More (46%) think disruption to customers is a barrier, compared to EMEA (22%).
 - More (35%) say disruption to sales and the revenue stream is a barrier, compared to EMEA (21%).
- In fact, organisations questioned in 2007 say more barriers apply to their organisation's DR plan testing, compared to previous years, and all barriers are selected by more organisations in 2007 than previously.

- Interestingly, there seems to be a false sense of security among those that have not yet tested their DR plan.

"We are sceptical about testing something unless we deem it fully necessary. If for some reason our plan didn't work, we would only like to discover this in the event of a disaster." USA, IT Manager, 1,000 employees, investment banking sector.

"I don't think we will have any barriers when we do it." Italy, IT Director, 550 employees, public sector.

"I don't think there are any barriers; we just haven't done it." USA, IT Manager, 1,500 employees, local and federal government.

Fire disaster scenario: [Section 3.18]

- When presented with a hypothetical scenario where a significant fire disaster occurs at their organisation and completely obliterates the main data centre, many organisations (66%) say they could achieve skeleton operations within a relatively short time frame of less than 12 hours.
- In contrast, the average time it would take to get things mostly back up and running is 5.3 days, and this is as long as 3 months in some organisations.
- Furthermore, the average time it would take to be able to get back to 100% normal operations is 19 days, and this can be as long as 18 months in some cases.
- However, only 16% of these organisations have ever had to execute their DR plan for real due to a natural disaster, such as a fire or a flood – and this group's estimates of getting back to skeleton operations are in line with those that have not experienced this type of disaster, but their estimates of getting back to 100% normal operations are longer (28 days), compared to those that have tested their DR plan (18 days).
- Interestingly, time estimates from EMEA IT managers are longer than those in the US when it comes to achieving skeleton operations, but the converse is true for getting things back to 100% normal operations with US IT managers being more pessimistic.
- Based on the average figures, countries that would take the longest to get back to 100% normal operations include the Netherlands, Germany, Sweden, Switzerland, the UK and the US, with the UK taking the longest.
- Since 2004, organisations' estimates for achieving skeleton operations have shortened, from an average of 3.2 days in 2004 to 0.8 days in 2007.
- But the converse is true for estimates for getting back to 100% normal operations, which was 6.6 days in 2004 and is now 19 days.
- This may be due to the increase in the frequency of testing and actual execution that has occurred between 2004 and 2007 – this is supported by the fact that 40-45% of organisations in 2004 admitted they did not know how long it would take to respond to such a disaster, compared to just 2% in 2007.

Real-time execution of the DR plan: [Sections 3.17 & 3.22]

- 1 in 2 organisations (48%) have had to execute for real their DR plan, either in full or in part.
- Indeed, 1 in 4 (26%) have had to execute it for 2 or more reasons; and 12% have had to do it for 3 or more.
- The most common circumstance for DR plan execution has been computer system failure, such as hardware and software failure (22%).
- This is followed in second place by 16% that have executed it for real due to natural disasters, such as fire and floods.
- Almost as many (15%) have executed it due to external computer threats, such as viruses and hackers.
- EMEA organisations have had to execute their DR plans for more of these reasons, compared to the US, especially:
 - Natural disasters, such as fire and floods (17%), compared to the US (8%).
 - Computer system failure (23%), compared to the US (14%).
 - IT problem management (10%), compared to the US (4%).
- But, more US organisations (22%) have executed their DR plan due to external computer threats, like viruses and hackers, compared to EMEA (14%).
- This means that natural disasters are as common as attacks from viruses and / or hackers, especially in EMEA, but not in the US.
- More organisations questioned in 2004 (51%) and 2007 (48%) have had to execute for real their DR plan, either in full or in part, compared to 2003 (33%).
 - More in 2004 (14%) and 2007 (16%) had to execute it due to natural disasters, compared to 2003 (7%).
 - More in 2004 (10%) and 2007 (9%) have implemented due to man-made disasters, compared to 2003 (2%).
 - More in 2004 (37%) and 2007 (22%) have implemented due to computer system failure, compared to 2003 (18%).
 - More in 2004 (13%) and 2007 (9%) have implemented due to internal computer threats, compared to 2003 (6%).
- In fact, 44% of organisations without a DR plan have experienced at least some sort of problem or disaster - indeed, 26% have experienced 2 or more and 11% have experienced 3 or more.
- The Top 3 disasters experienced by those without a DR plan are almost identical to the list for those with a DR plan:
 1. Computer system failure (22%)
 2. External computer threats from viruses and hackers (18%)
 3. Natural disasters like fire and floods (17%)

Suppliers – an Achilles heel? [Section 3.19]

- For many organisations, suppliers are integral to the smooth running of the business, yet 29% of these large organisations do not ask to see the BC and DR plans of any of their third party suppliers, as they assume they have adequate plans.

- Another 4% are unsure about the degree to which such plans of suppliers are given consideration by their organisation.
- Only 28% routinely ask to see the BC and DR plans of all suppliers for the whole of their organisation before they start work with them.
- Another 34% routinely ask technology suppliers this question, and 12% ask it to outsourced managed service providers.

2. Research Methodology

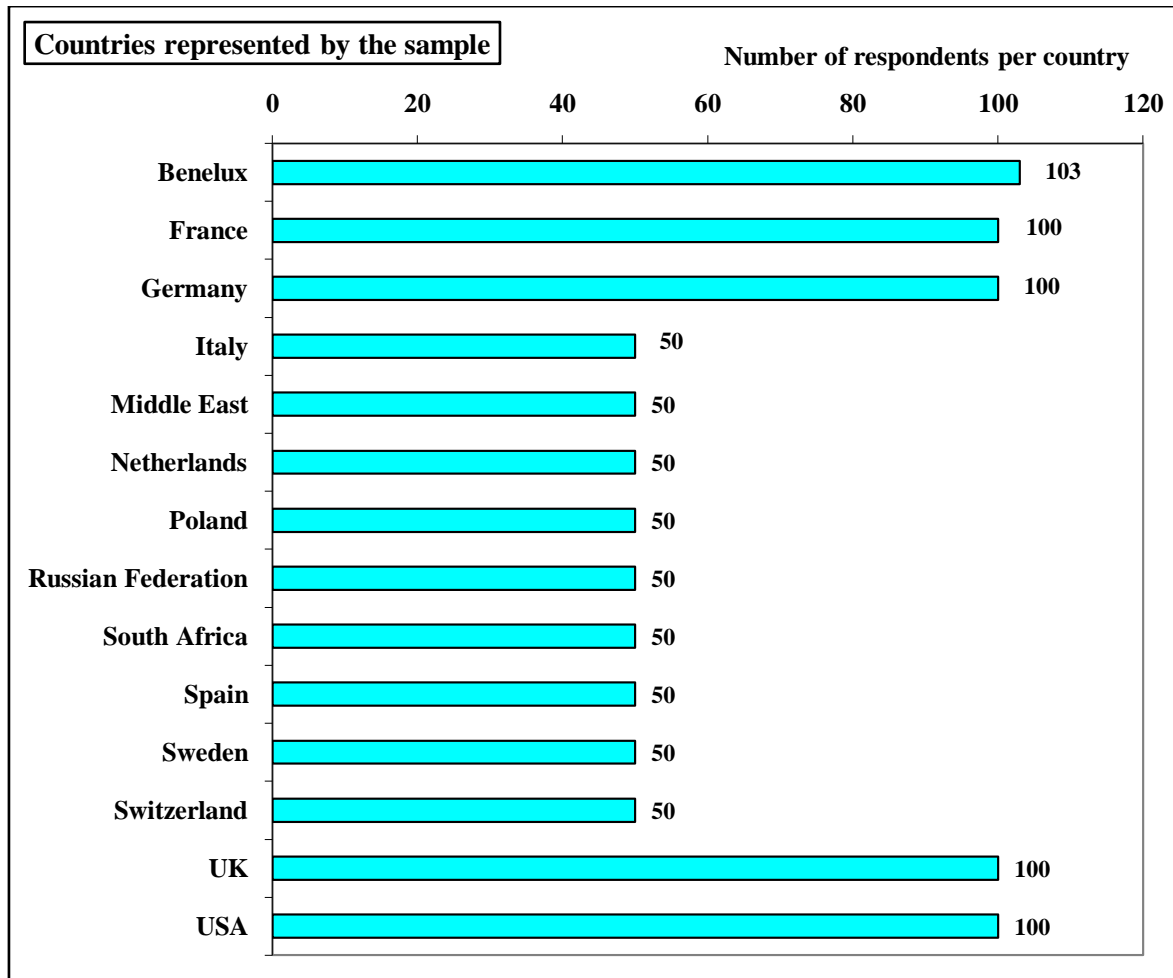
2.1 Overview:

This report was commissioned by the Symantec Corporation and details qualitative and quantitative research with IT managers in large organisations across the US, 11 European countries, the Middle East and South Africa.

The objective of the qualitative research was to gain insight and understanding into some of the more complicated issues associated with disaster recovery. These issues were subsequently quantified by collecting a larger sample from the same universe. This report draws together and reports the findings from these surveys which represent a total of 1088 interviews.

2.2 Quantitative Research:

903 interviews were collected with IT managers who have responsibility for and are involved in the management of their organisation’s disaster recovery plan in organisations with >500 employees. The resulting sample includes a variety of industry sectors.



Prior to being interviewed, all respondents confirmed that their organisation has 500 or more employees worldwide, and that they are responsible for the organisation's disaster recovery plan, as well as being involved in the day-to-day management of the plan.

In addition, 148 organisations that do not have a DR plan were also interviewed and asked why they do not have a DR plan. These represent 14% of the total sample.

Both these sub-samples are balanced according to country, with more respondents from the US, UK, Germany and France to represent the larger economies of these countries. In addition, 50 interviews were collected in the Netherlands and another 53 in Belgium and Luxemburg. In the report, the Netherlands data is shown as a single country, but it is also grouped with Luxemburg and Belgium and described as Benelux.

Interviews were conducted by Dynamic Markets Limited between 24th July and 15th August 2007. Before and during the interviews, respondents were not aware that Symantec had commissioned the research.

Comparative Analysis:

The findings of the quantitative survey have been analysed and compared according to region (i.e. USA versus EMEA) and country. In addition, some of the questions from this survey were also posed to a similar sample in 2004 and 2003. Where appropriate, answers between the 3 data sets have been compared.

Where any interesting differences exist that are significant at a 95% confidence level for these elements, they are described accordingly in this report. The following statistical confidence at a 95% level has been used when analysing the data.

Table 1: Margin of error at a 95% confidence level:

Sample size	50	100	200	300	400	500	1000
5% or 95%	±6.2%	±4.4%	±3.1%	±2.5%	±2.2%	±1.9%	±1.4%
10% or 90%	±8.5%	±6.0%	±4.2%	±3.5%	±3.0%	±2.7%	±1.9%
25% or 75%	±12.5%	±8.7%	±6.1%	±5.0%	±4.3%	±3.9%	±2.7%
50%	±14.1%	±10%	±7.1%	±5.8%	±5.0%	±4.5%	±3.2%

Table 2: Weighted sub-sample sizes for those with a DR plan (n):

Countries	n=	Global regions	n=	Trend data	n=
Benelux	103	EMEA	803	2007	903
France	100	USA	100	2004	1074
Germany	100			2003	850
Italy	50				
Middle East	50				
Netherlands	50				
Poland	50				
Russia	50				
South Africa	50				
Spain	50				
Sweden	50				
Switzerland	50				
UK	100				
USA	100				

Table 3: Weighted sub-sample sizes for those without a DR plan (n):

Countries	n=	Global regions	n=	Trend data	n=
Benelux	16	EMEA	131	2007	148
France	17	USA	17	2004	173
Germany	17			2003	140
Italy	8				
Middle East	8				
Netherlands	8				
Poland	8				
Russia	8				
South Africa	8				
Spain	8				
Sweden	8				
Switzerland	8				
UK	17				
USA	17				

Throughout this report, where any numbers do not add up to 100%, it is either because respondents were allowed to select more than one tick-box option in the question, or because of minor rounding errors, which should be ignored.

2.3 Qualitative Research:

For the initial qualitative phase of the project, 37 respondents were interviewed, as summarised in the table below:

Table 4: Breakdown of qualitative sample:

Country	Sectors	Totals
Germany	3 public; 2 automotive; 1 manufacturing	6
Italy	3 public; 3 banking	6
Middle East	4 public; 2 banking	6
Russia	3 public; 3 power and energy	6
UK	4 public; 2 banking; 1 power and energy	7
USA	3 public; 2 investment banking; 1 local and federal government	6
Totals		37

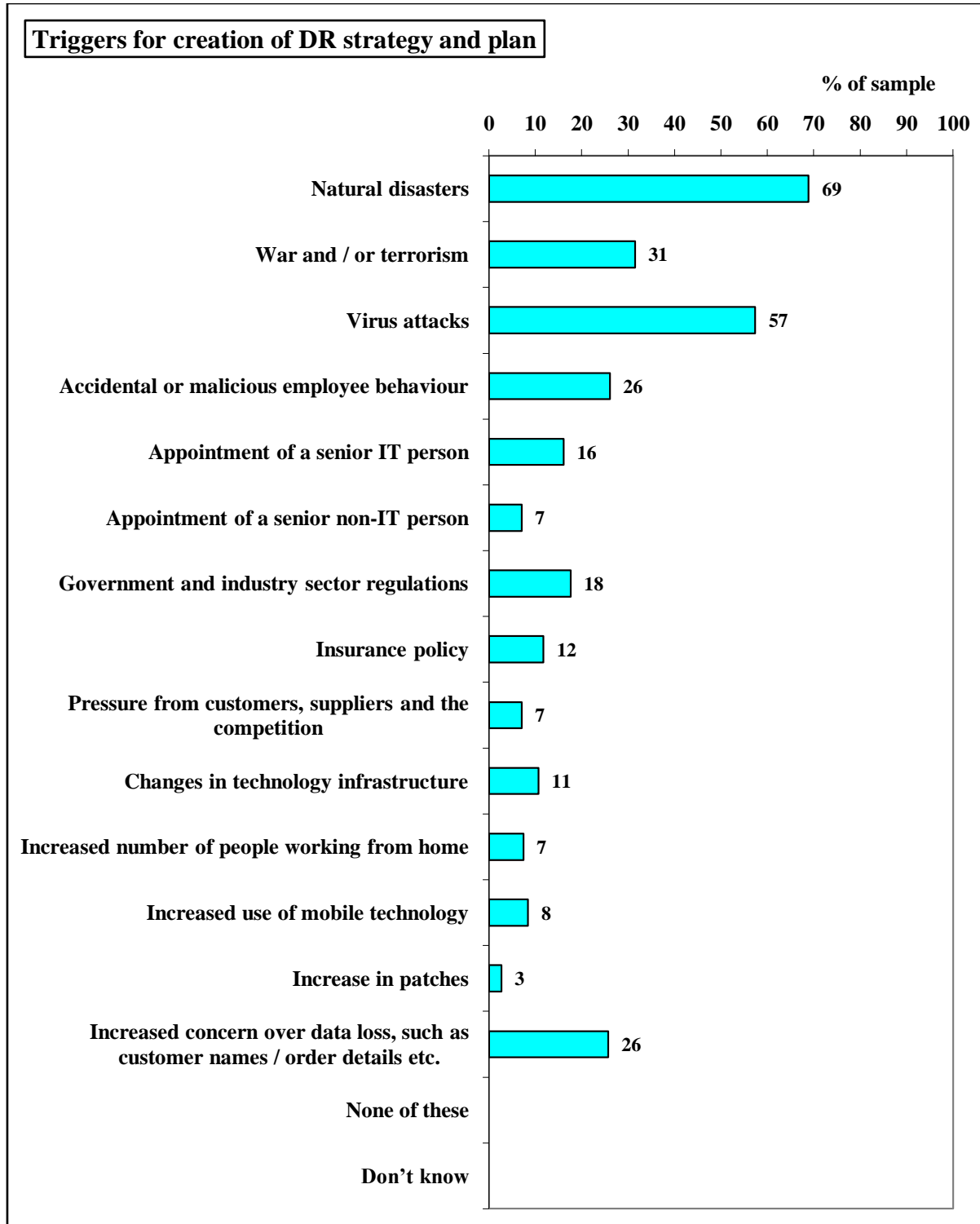
The average number of employees for the sample is 8,697, but this ranges from 500 to 160,000. All organisations have a disaster recovery plan.

Prior to being interviewed, all respondents confirmed that their organisation has 500 or more employees worldwide, and that they are responsible for the organisation's disaster recovery plan, as well as being involved in the day-to-day management of the plan.

Interviews were conducted by telephone between June 26th and July 11th 2007 by Dynamic Markets and lasted on average for 10-15 minutes. Before and during the interviews, respondents were not aware that Symantec had commissioned the research.

3. Key Findings

3.1 Which of the following prompted your organisation to first create a disaster recovery strategy and plan?



- All organisations with a DR plan were prompted by at least 1 of these issues to create their DR plan and strategy.

- Indeed, 83% were prompted by more than 1 of these; and 57% were prompted by 3 or more [not shown].
- The Top 3 issues that have prompted organisations to create a DR plan and strategy are:
 1. Natural disasters (69%)
 2. Virus attacks (57%)
 3. War and / or terrorism (31%)
- In addition, 26% of organisations were prompted to create a DR plan and strategy by accidental or malicious employee behaviour, and as many (26%) reacted to increased concerns over data loss, such as customer names / order details etc.
- Government and industry sector regulations (18%) have also been important.
- New appointments to the organisation meant the creation of a DR plan for 16% of organisations with a new senior IT person, and for 7% of organisations with a new senior non-IT person.
- 12% have created a DR plan because of an insurance policy.
- Changes in technology have prompted 11% of organisations, whereas 3% were triggered by an increase in patches.
- Another 8% say the increased use of mobile technology played a part, whereas 7% say the increased number of people working from home was a factor.
- Only 7% of organisations created a DR plan and strategy due to pressure from customers, suppliers and their competition.

"We had previously suffered a major blackout which led to the loss of data. This led us to build a DR plan." Germany, IT Director, 500 employees, automotive sector.

"We created it to protect our patients' data." Germany, IT Manager, 2,500 employees, public sector.

"The Bank of Italy legislates that we must have such a plan in place due to the nature of the information held by our business." Italy, IT Manager, 3,000 employees, banking sector.

"Due to political instability within our country, it has become compulsory for us to protect our customers in this way." Israel, IT Manager, 500 employees, banking sector.

"It was the introduction of new policies and regulations by the government that made us take action." Russia, IT Director, 2,330 employees, power and energy sector.

"Weather conditions; namely heat and the cold." Russia, IT Director, 3,450 employees, power and energy sector.

"The DRP is seen as a must for a modern organisation of this size. The management takes this matter seriously, in order to sustain the organisation's safety and public image. Although, our reputation is not as sensitive a matter as for financial services companies, for example." Russia, IT Director, 575 employees, public sector.

"Generally, we were responding to a demand from our clients and partners." Russia, IT Director, 510 employees, public sector.

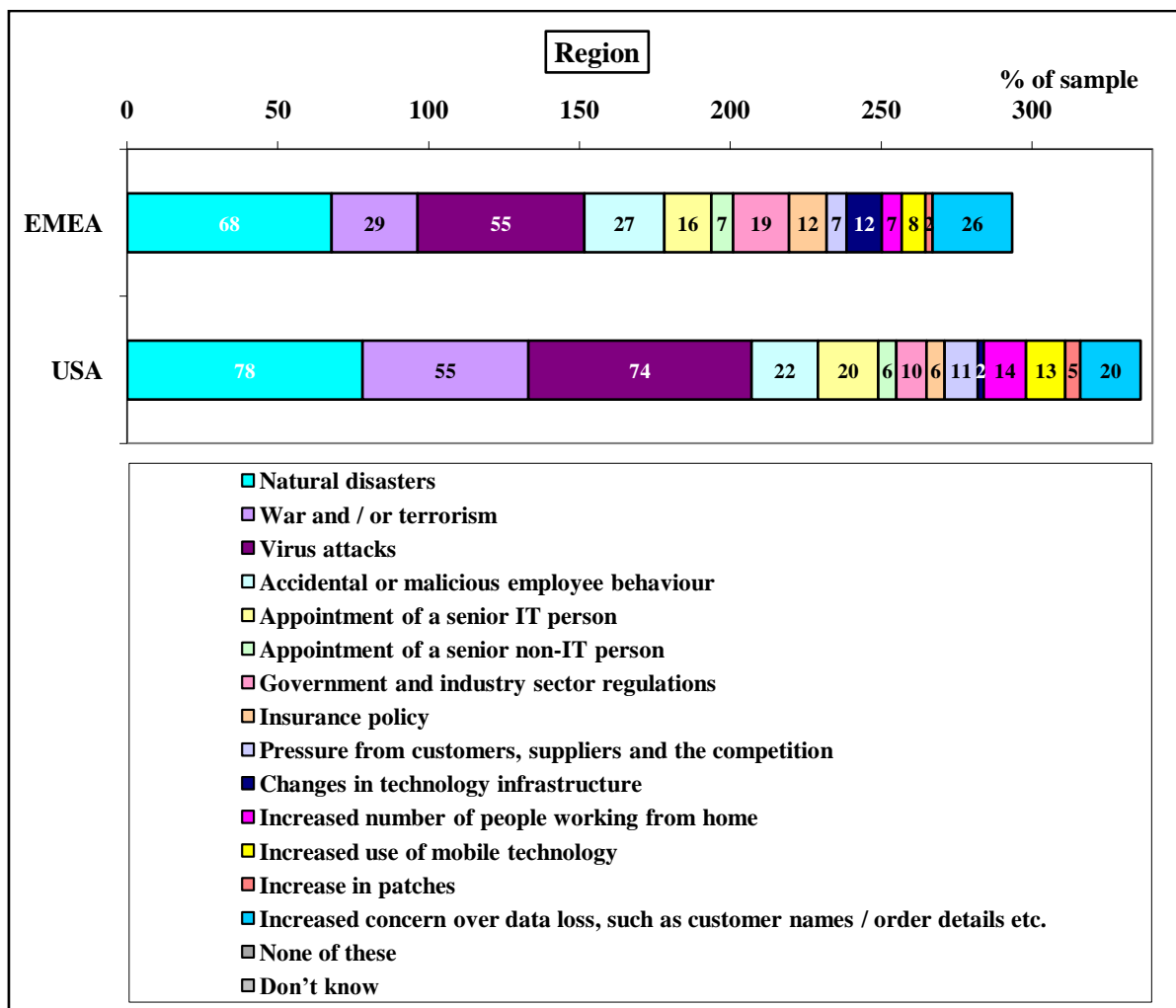
"We have always had some documents about disaster recovery, but recently there has been an auditing requirement and insurer's requirement and also because of our own standard ITIL." UK, IT Manager, 600 employees, public sector.

"A combination of good business practice and regulatory requirement." UK, Head of IT, 160,000 employees, banking sector.

"After the 9/11 attacks, we felt that the security of our organisation needed to be improved to protect the data and sensitive information of our clients." USA, IT Manager, 1,000 employees, investment banking sector.

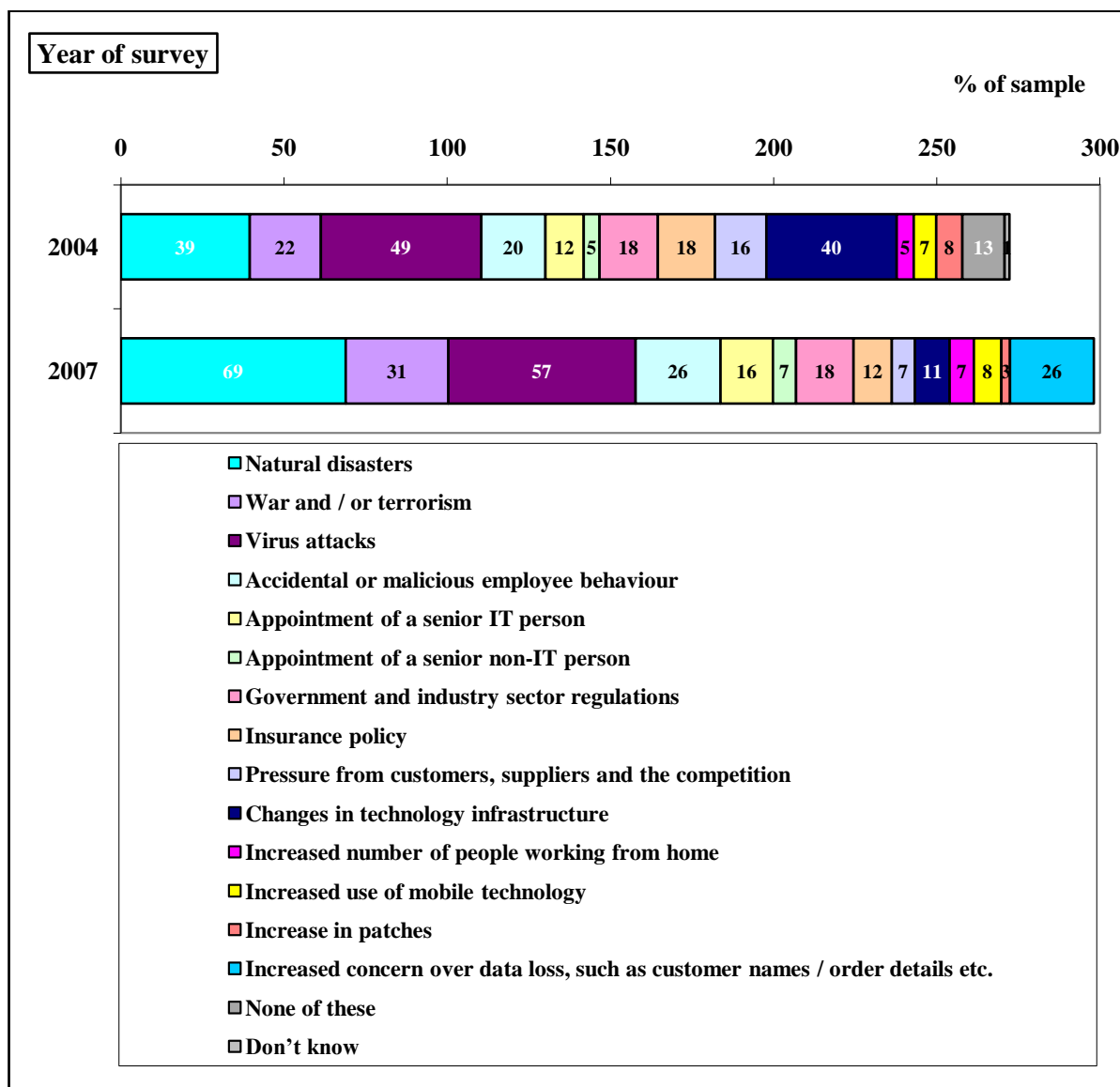
"After a series of severe floods within our area, we decided to create a disaster recovery plan." USA, IT Manager, 1,800 employees, investment banking sector.

"After September 11th, we decided we needed to be sure our data and information are recoverable and safe." USA, IT Manager, 3,500 employees, public sector.



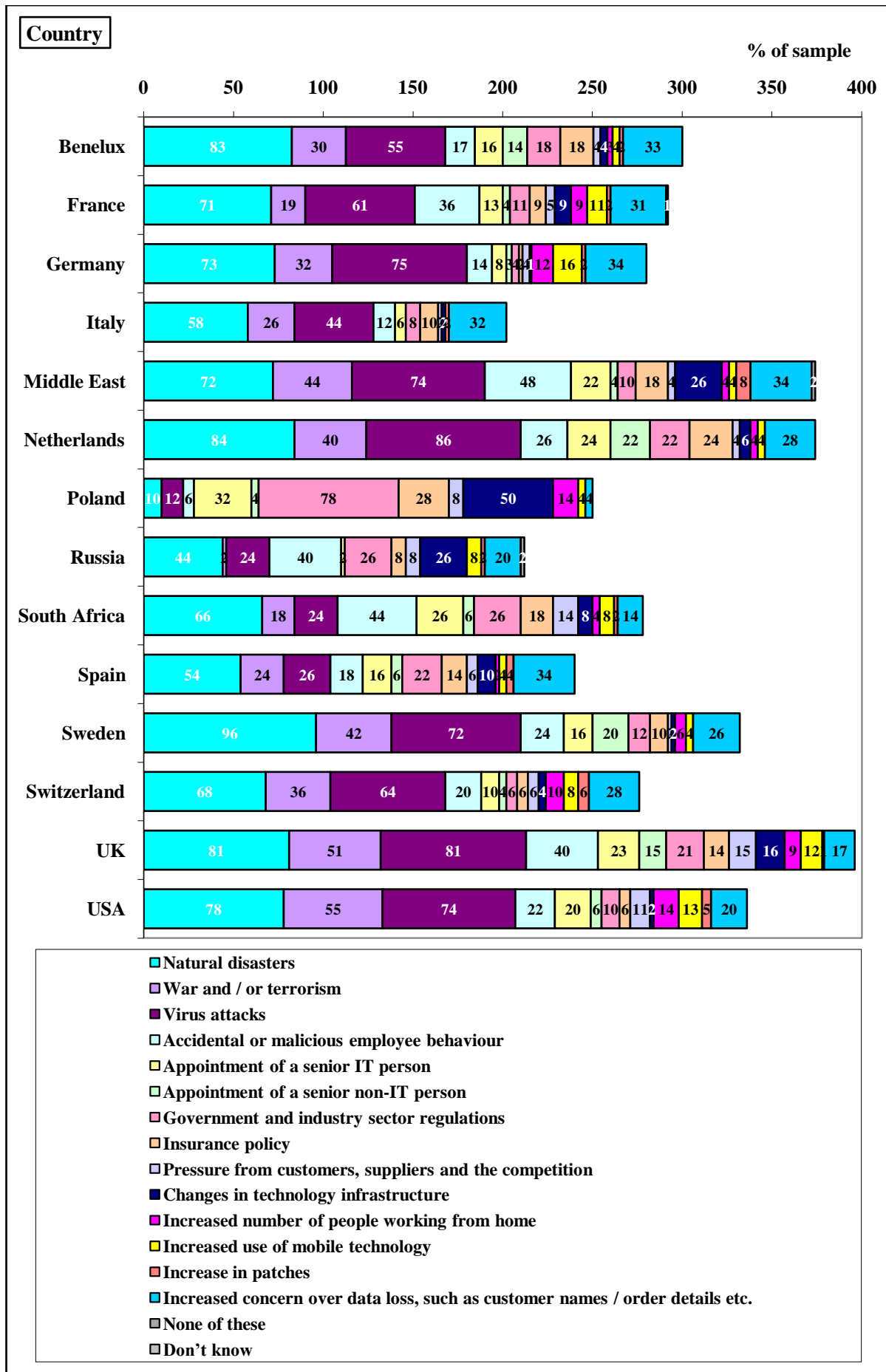
- Overall, US organisations say more of these factors prompted them to first create a DR plan and strategy, compared to EMEA organisations (i.e. length of bars in the above chart).
- Indeed, more US organisations (70%) were prompted to create a DR plan and strategy by 3 or more of these issues, compared to EMEA organisations (56%) [not shown].
- In detail, more US organisations (78%) were prompted to create a DR plan and strategy by natural disasters, compared to EMEA organisations (68%).
- Also, more US organisations (55%) were prompted by war and / or terrorism, compared to EMEA organisations (29%).
- In addition, more US organisations (74%) were prompted by virus attacks, compared to EMEA organisations (55%).

- But, more EMEA organisations (19%) were prompted by Government and industry sector regulations, compared to US organisations (10%).
- And, more EMEA organisations (12%) were prompted by changes in technology infrastructure, compared to US organisations (2%).
- However, more US organisations (14%) were prompted by the increased number of people working from home, compared to EMEA organisations (7%).

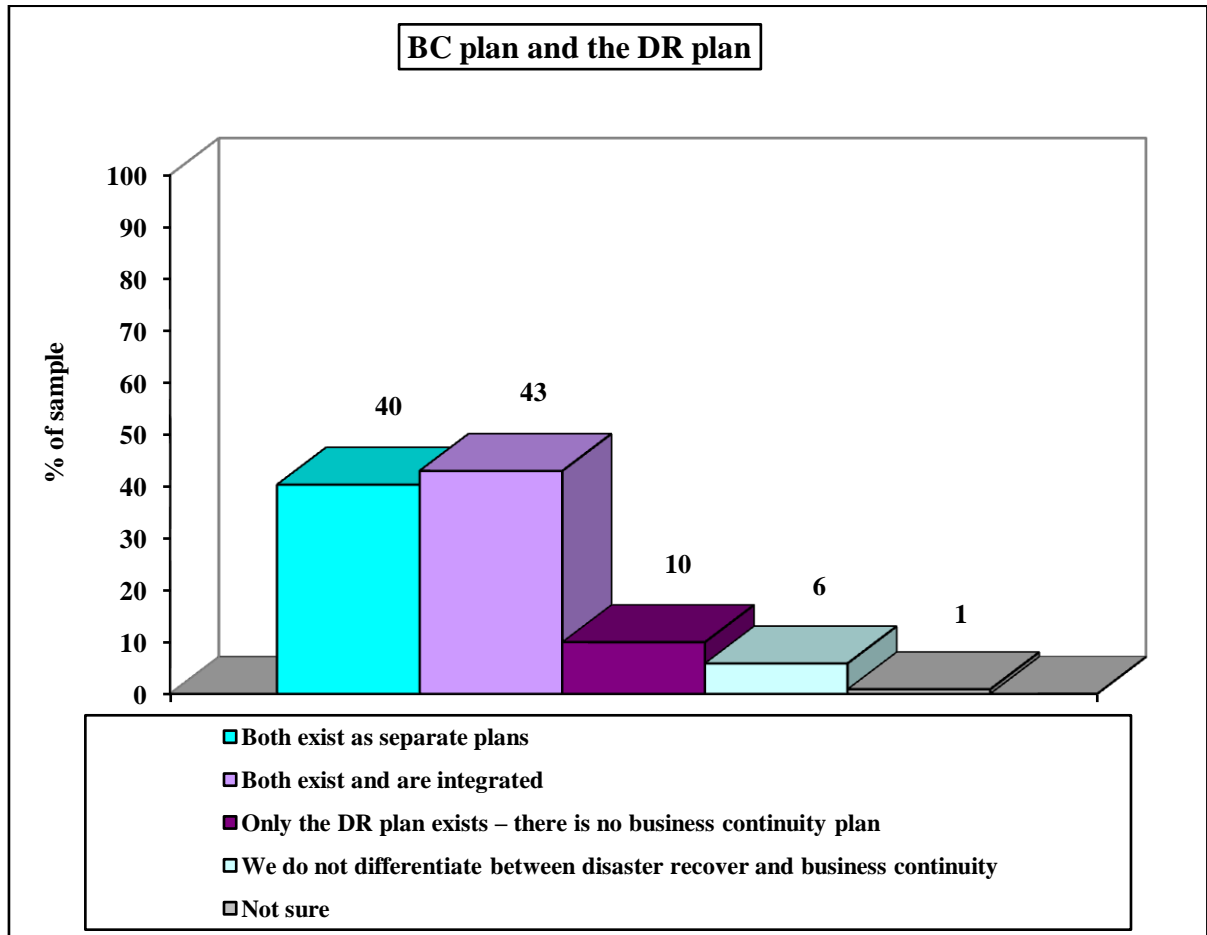


- More organisations questioned in 2007 (69%) were prompted to create a DR plan and strategy by natural disasters, compared to organisations questioned in 2004 (39%).
- And, more organisations questioned in 2007 (31%) were prompted to create a DR plan and strategy by war and / or terrorism, compared to those questioned in 2004 (22%).
- Also, more organisations questioned in 2007 (57%) were prompted by virus attacks, compared 2004 (49%).
- In addition, more organisations questioned in 2007 (26%) were prompted by accidental or malicious employee behaviour, compared to 2004 (20%).

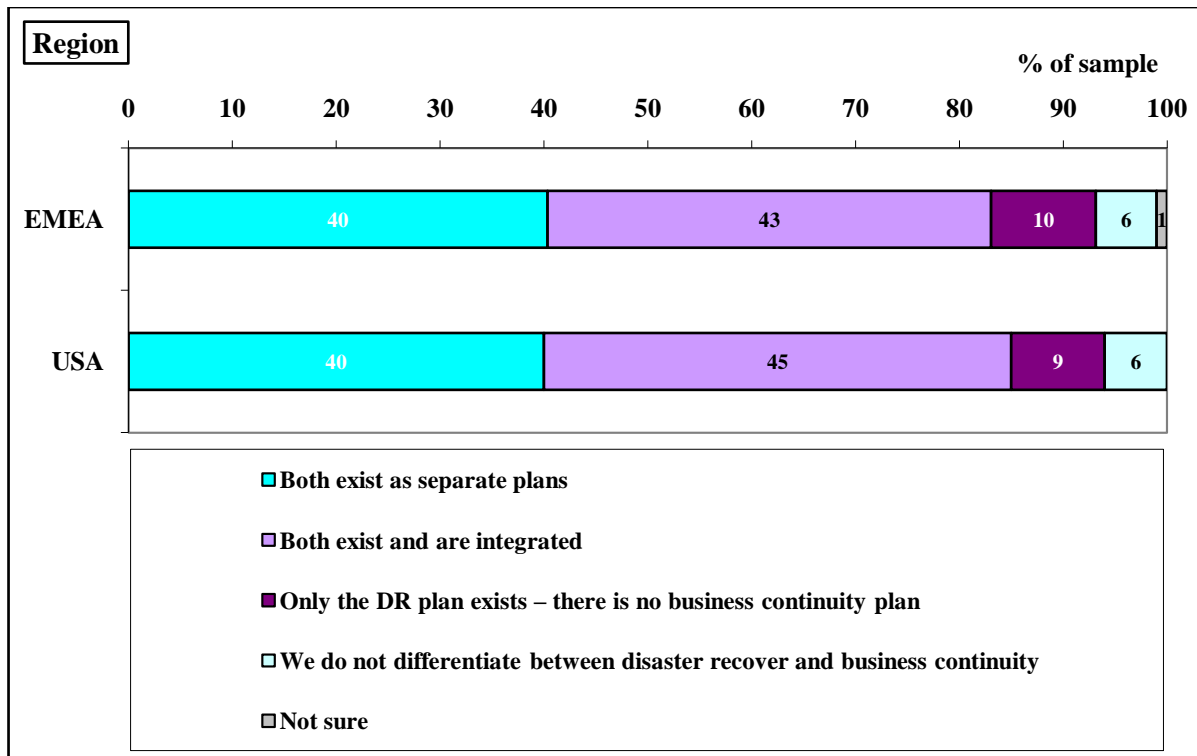
- Yet, more organisations questioned in 2004 (18%) were prompted by an insurance policy, compared to 2007 (12%).
- And, more organisations questioned in 2004 (16%) were prompted by pressure from customers, suppliers and their competition, compared to 2007 (7%).
- Also, more organisations questioned in 2004 (40%) were prompted by changes in technology, compared to 2007 (11%).
- Whereas, more organisations questioned in 2004 (8%) were prompted by an increase in patches, compared 2007 (3%).
- Finally, more organisations questioned in 2004 (13%) were not prompted to create a DR plan and strategy by any of these, compared to organisations questioned in 2007 (zero).



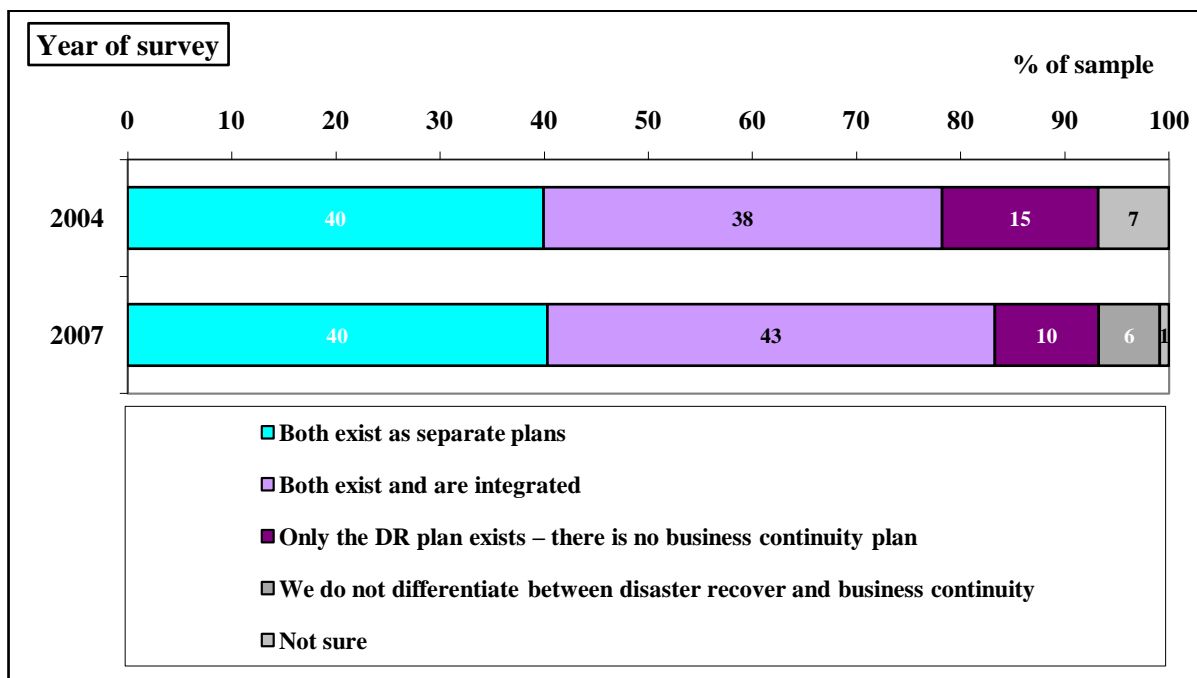
3.2 In which of the following ways does your business continuity (BC) plan relate to your disaster recovery (DR) plan?



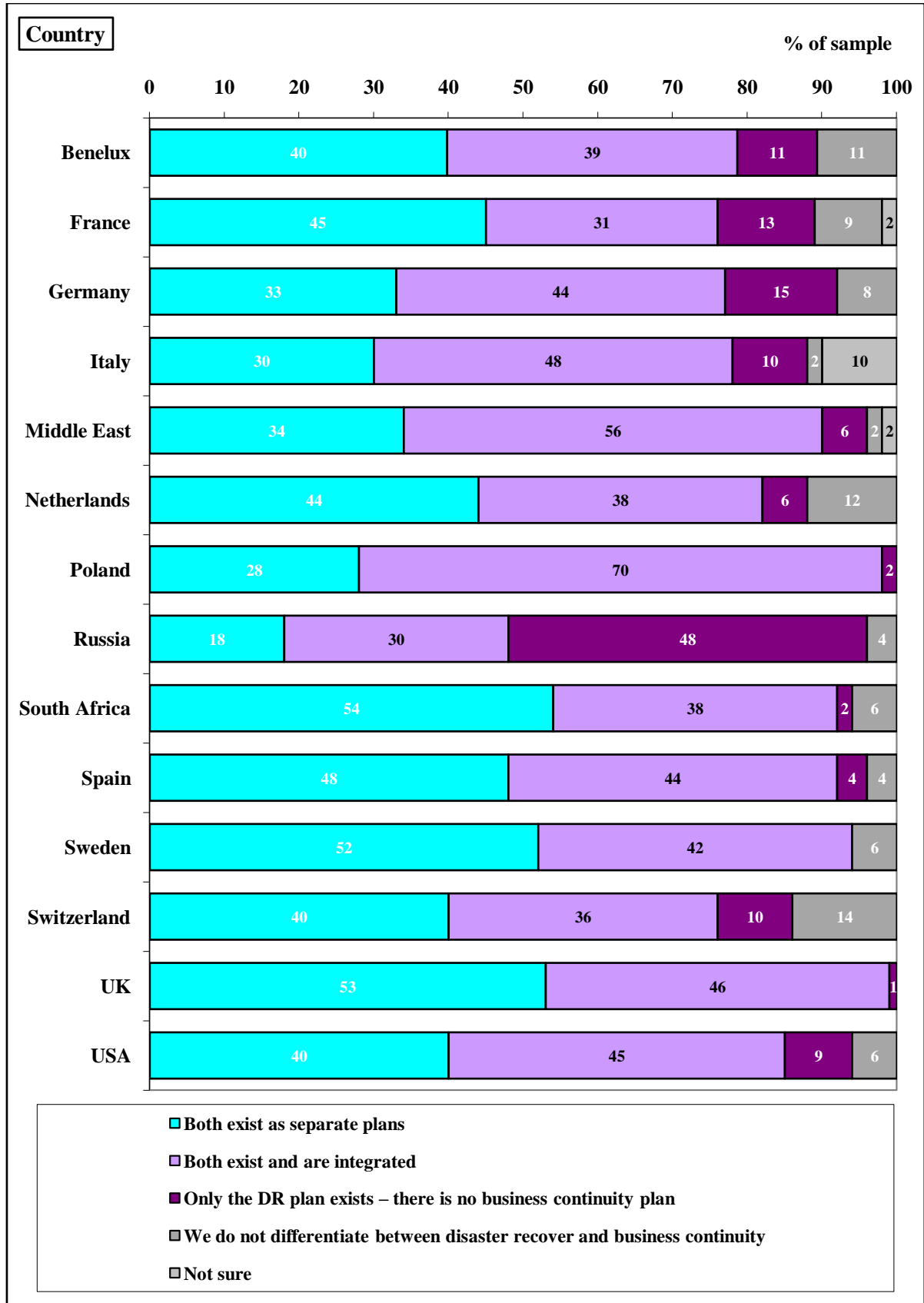
- 10% of organisations have a DR plan only, but not a BC plan.
- In addition, 40% have a DR plan and a BC plan, but they exist as separate plans.
- In contrast, 43% of organisations have a DR plan that is integrated with the BC plan.
- But 6% of organisations do not differentiate between disaster recovery and business continuity.
- 1% do not know how the DR plan relates to the BC plan.



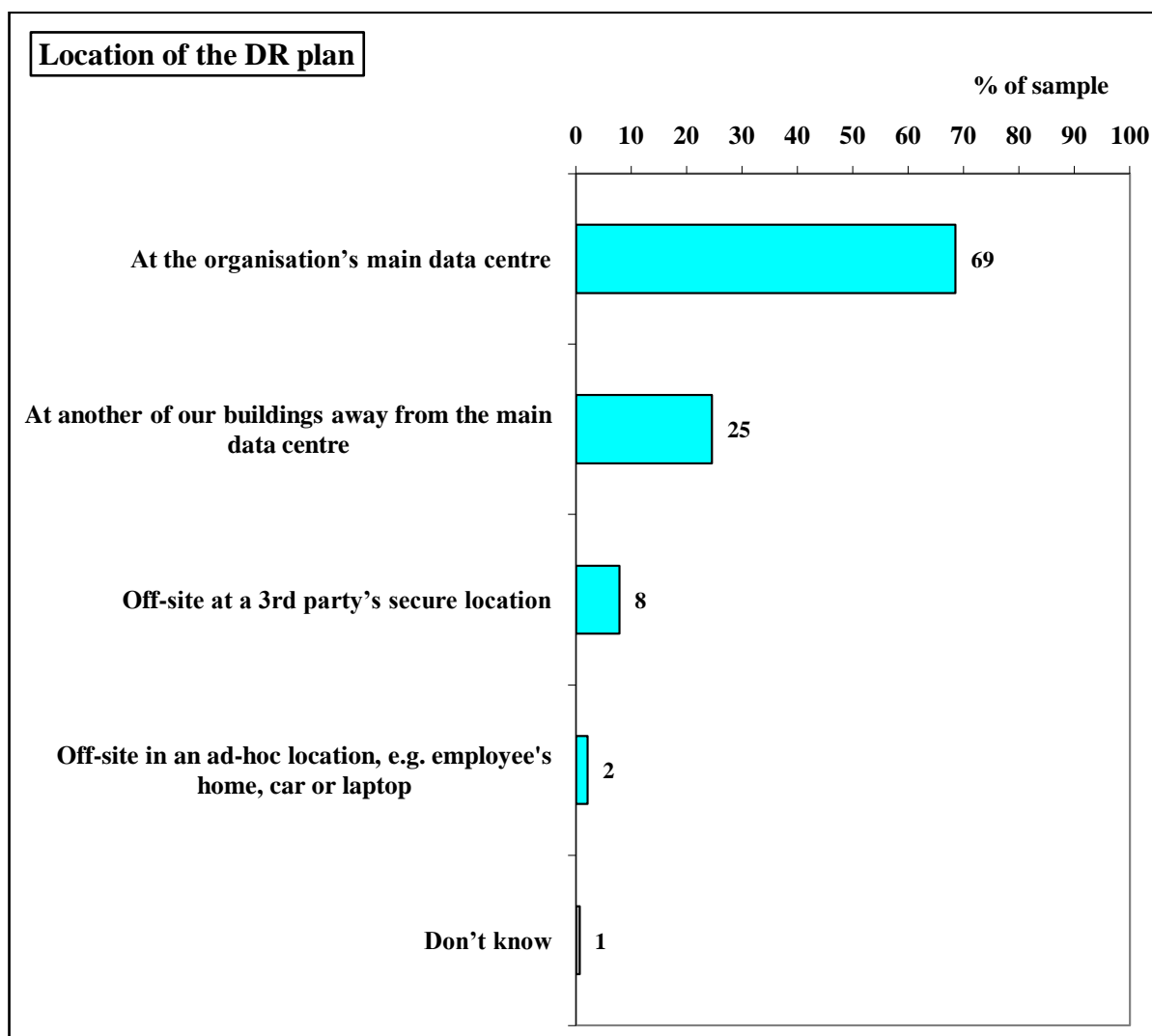
- Statistically, there is no significant difference according to region and how the BC relates to the DR plan.



- More organisations questioned in 2004 (15%) had a DR plan and did not have a BC plan, compared to organisations questioned in 2007 (10%).
- But, more organisations questioned in 2007 (43%) have a DR plan that is integrated with the BC plan, compared to those questioned in 2004 (38%).



3.3 Where is the disaster recovery plan located?



- 69% of organisations say their DR plan is located in the main data centre.
- In fact, 65% of the sample ONLY keep the DR plan in the organisation's main data centre [not shown].
- Just 25% keep the DR plan at another of the organisation's buildings away from the main data centre.
 - Distances to such a location from the main data centre range from less than 1 km to 5000 km with an average of 190 km, but a median of just 30 km; furthermore, 37% say the DR plan is located within 1-10 km, and another 21% say it is located within 11-50 km; only 18% say it is located more than 100 km away from the main data centre building [not shown].
- Only 8% keep the DR plan located off-site at a 3rd party's secure location.
 - Distances to such a location from the main data centre range from 1-2000 km with an average of 341 km, but a median of just 100 km; furthermore, 10% say the DR plan is located within 1-10 km, and another 31% say it is located within 11-50 km; but 44%

say it is located more than 100 km away from the main data centre building [not shown].

- Only 2% keep their DR plan off-site in an ad-hoc location, such as an employee’s home, car or on a laptop.
- 1% are not sure where their DR plan is located.
- 96% of organisations keep their DR plan in just 1 of these locations – and only 4% keep the plan in 2 locations – none of the sample keep them in 3 or more of these locations [not shown].
- Furthermore, only 3% keep their plan in the main data centre and also at another of their organisation’s buildings away from the main data centre [not shown].
- Also, less than 1% keep their plan in the main data centre and also off-site at a 3rd party’s secure location [not shown].
- And only 1% keep their plan in the main data centre and also in ad-hoc locations, such as an employee’s home, car or on a laptop [not shown].

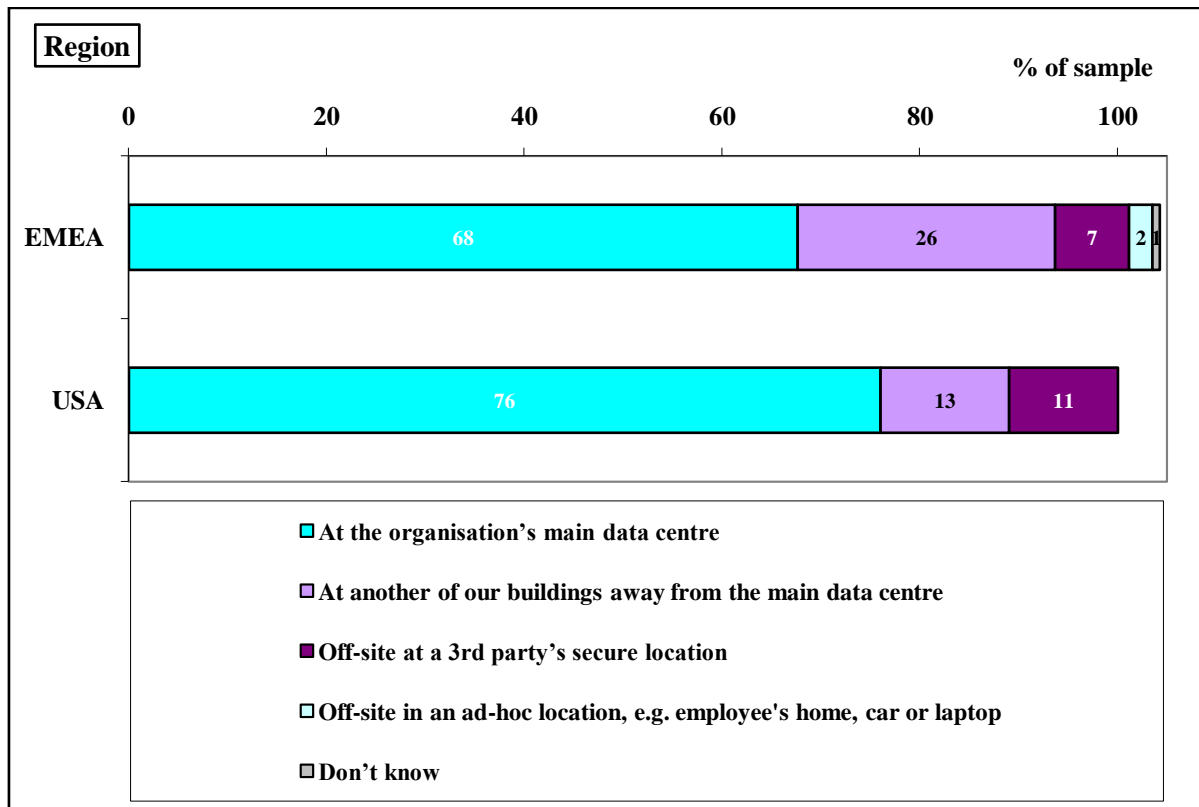


Table 5: Average distances to main data centre: regions

Region	Another of the organisation's buildings	Off-site at a 3 rd party's secure location
EMEA	197 km	342 km
USA	80 km	334 km

- More US organisations (76%) only keep the DR plan in the organisation’s main data centre, compared to EMEA organisations (68%) [not shown].

- And, more EMEA organisations (26%) keep the DR plan at another of the organisation’s buildings away from the main data centre, compared to US organisations (13%).
- And, more EMEA organisations (4%) keep the plan in 2 of these locations, compared to US organisations (zero) [not shown].



Table 6: Average distances to main data centre: year of survey

Year of survey	Another of the organisation’s buildings	Off-site at a 3 rd party’s secure location
2003	108 km	74 km
2004	133 km	167 km
2007	190 km	340 km

- More organisations questioned in 2004 (26%) and 2007 (25%) keep the DR plan at another of the organisation’s building away from the main data centre, compared to those questioned in 2003 (20%).
- But, more organisations questioned in 2003 (15%) and 2004 (18%) keep the DR plan located off-site at a 3rd party’s secure location, compared to organisations questioned in 2007 (8%).
- More organisations questioned in 2003 (62%) and 2007 (65%) only keep the DR plan in the main data centre, compared to those questioned in 2004 (53%) [not shown].

- But, more organisations questioned in 2004 (7%) keep their DR plan in the main data centre and also at another of their organisation's buildings, compared to 2003 and 2007 (both 3%) [not shown].
- However, more of those questioned in 2003 (3%) and 2004 (4%) keep their DR plan in the main data centre and also off-site at a 3rd party's secure location, compared to 2007 (zero) [not shown].
- More organisations questioned in 2003 (5%) and 2004 (3%) were not sure where their plan was located, compared to 2007 (1%).

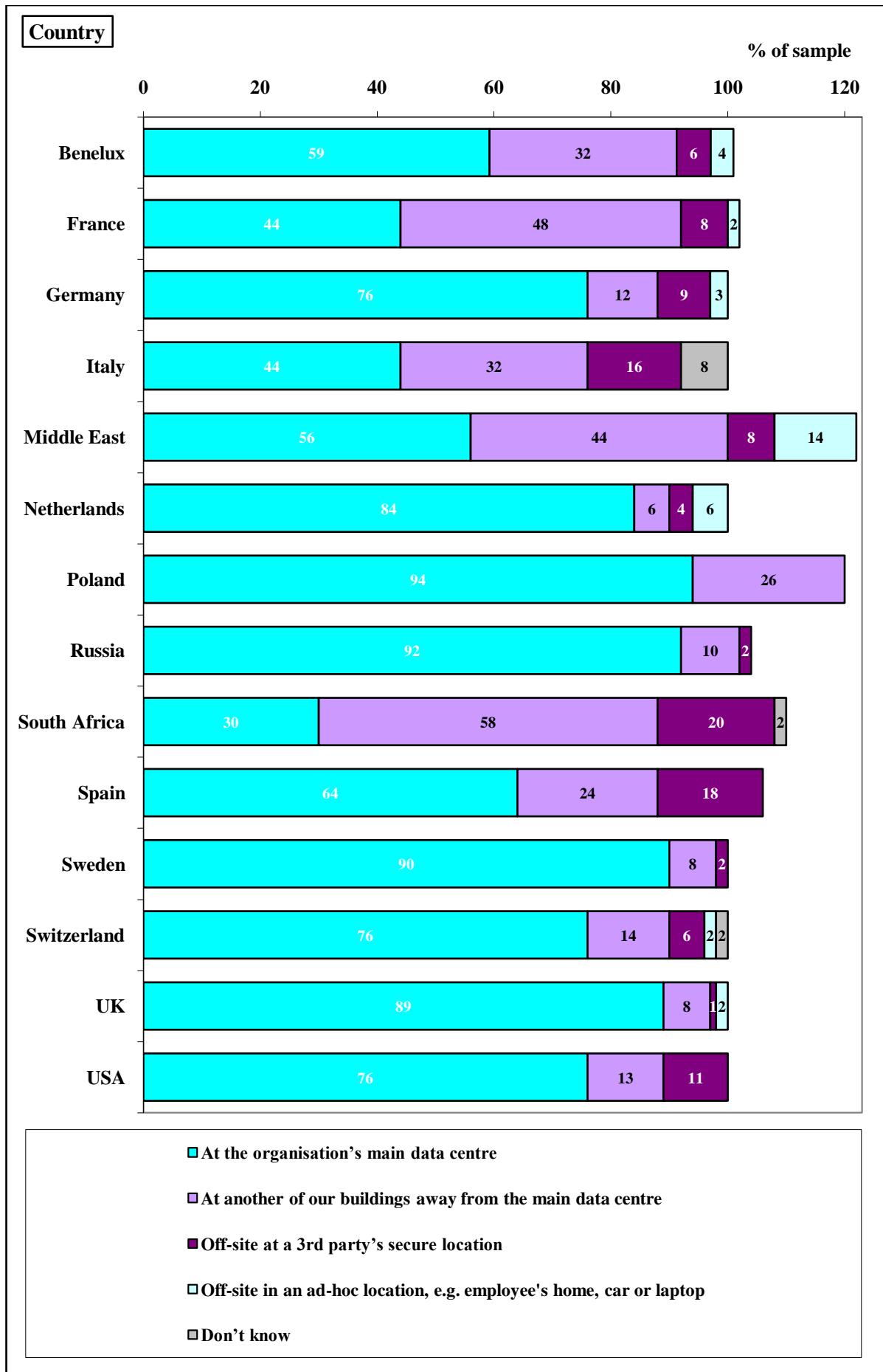
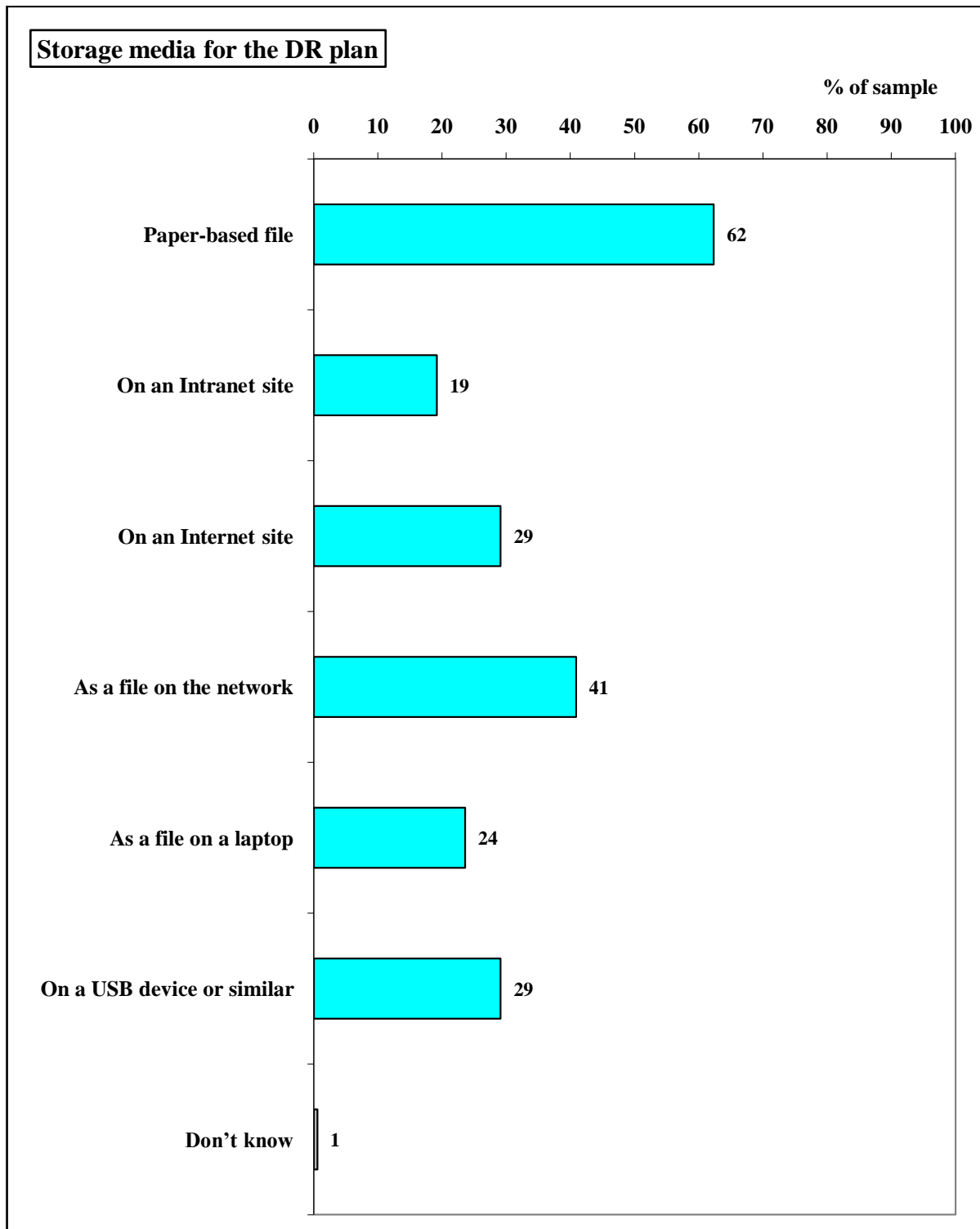


Table 7: Average distances to main data centre: countries

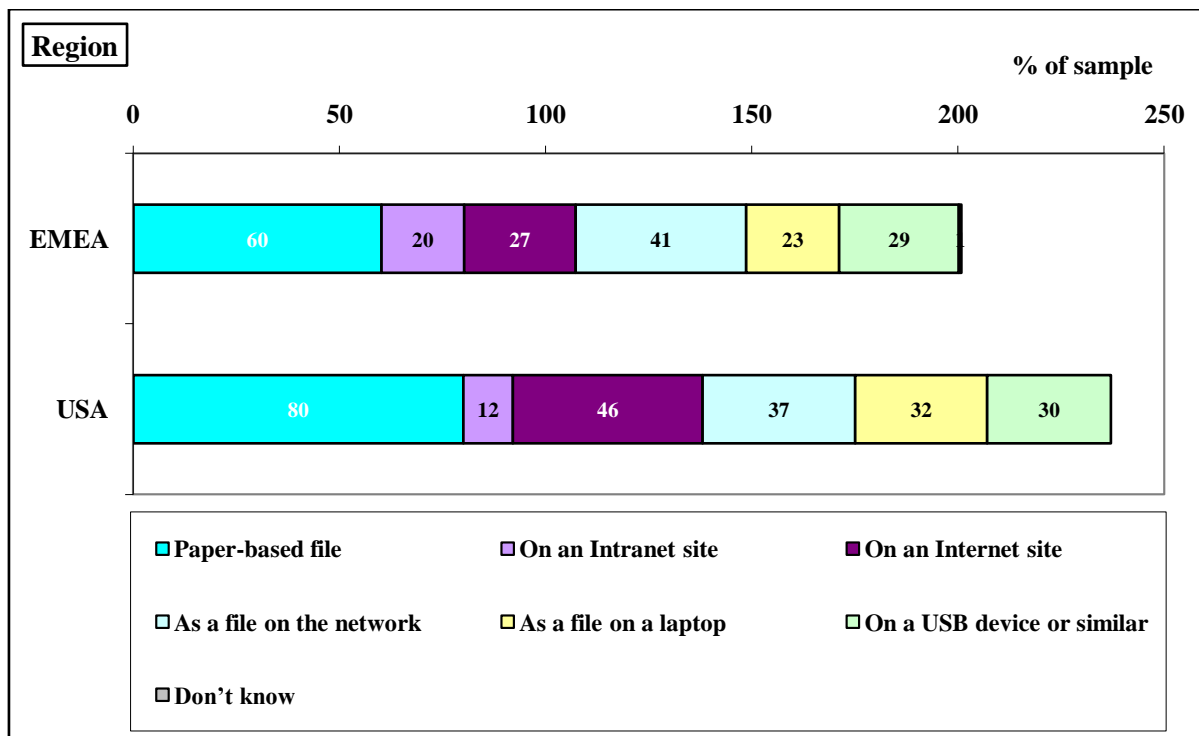
Country	Another of the organisation's buildings	Off-site at a 3rd party's secure location
Benelux	79 km	341 km
France	132 km	758 km
Germany	537 km	478 km
Italy	110 km	583 km
Middle East	116 km	60 km
Netherlands	67 km	20 km
Poland	75 km	1500 km
Russia	116 km	n/a
South Africa	40 km	1000 km
Spain	115 km	33 km
Sweden	1761 km	246 km
Switzerland	1346 km	200 km
UK	104 km	833 km
USA	80 km	100 km

3.4 On which of the following media is the DR plan located?

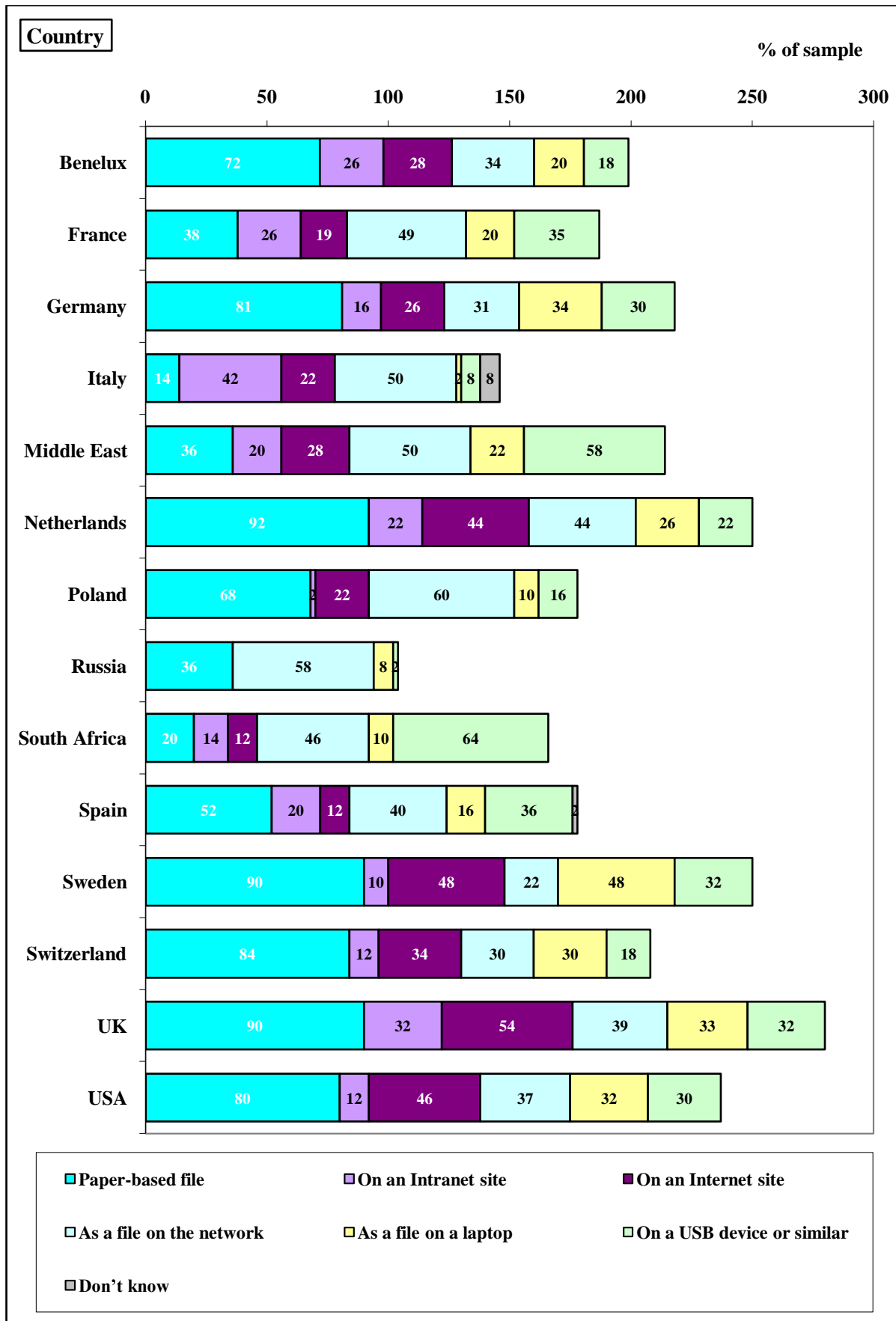


- 62% of organisations say their DR plan takes the form of a paper-based file.
- Another 41% store it as a file on the network.
- 29% have it stored on a USB device or similar, and as many store it on an Internet site (29%).

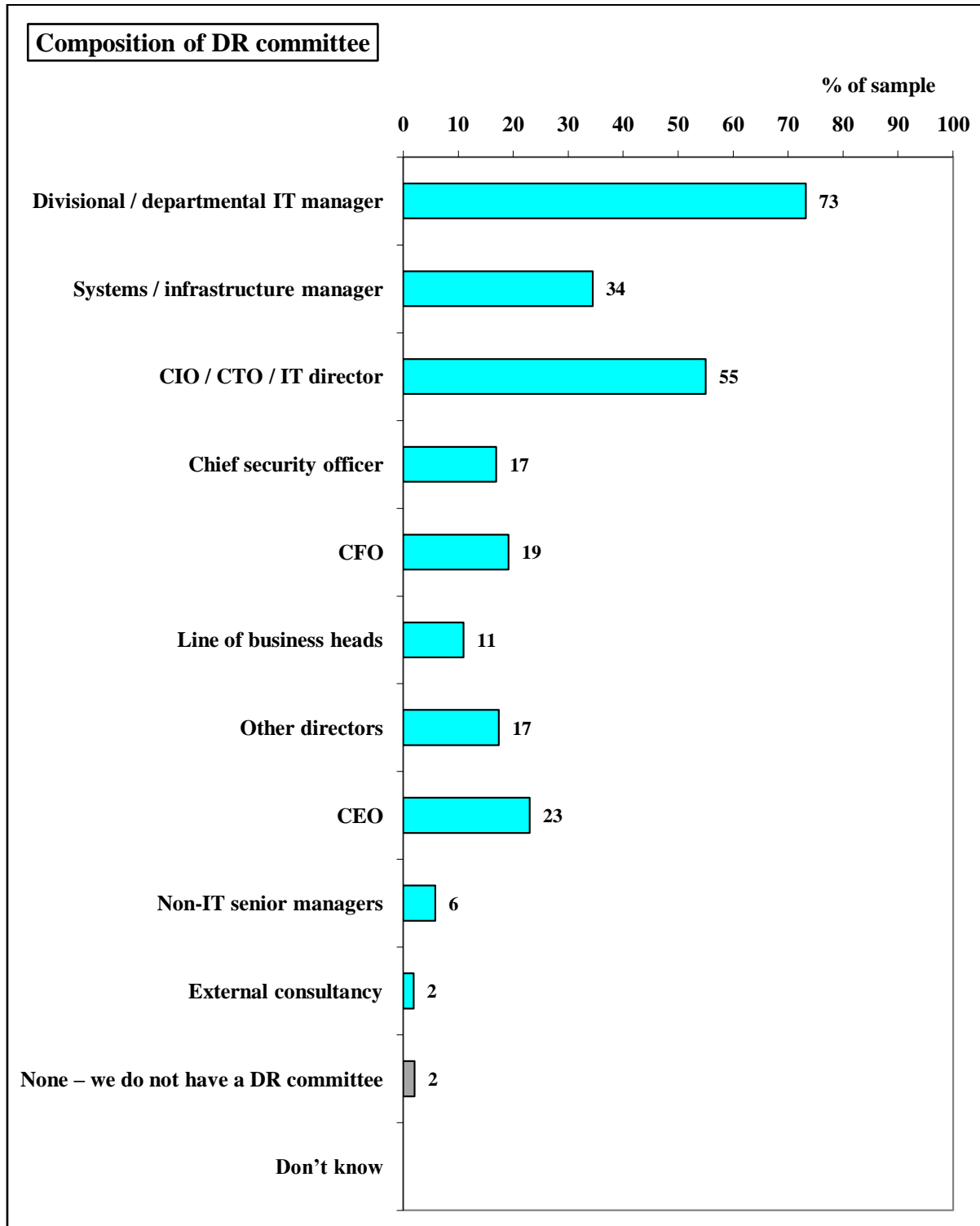
- 24% store the DR plan as a file on a laptop and 19% store it on an Intranet site.
- 66% of organisations store the DR plan across more than 1 of these media; almost a third (31%) store it across 3 or more, but only 1% store it across 5 or more [not shown].
- But 8% of organisations ONLY keep their plan as a paper-based version [not shown].
- 2% keep only paper-based and Intranet versions [not shown].
- Similarly, only 1% keep the plan as only paper-based and Intranet versions, along with a copy on the network [not shown].
- Finally, just 1% only keep their plan as a file on a laptop or USB device [not shown].
- 1% are not sure of the media on which the DR plan is located.



- Overall, US organisations say their DR plan is located on more of these media, compared to EMEA organisations (i.e. length of bars in the above chart).
- In addition, more US organisations (78%) store the DR plan across more than 1 of these media, compared to EMEA organisations (65%) [not shown].
- Furthermore, more US organisations (44%) store the DR plan across 3 or more different media, compared to EMEA organisations (30%) [not shown].
- In detail, more US organisations (80%) say their DR plan takes the form of a paper-based file, compared to EMEA organisations (60%).
- Also, more US organisations (46%) store the DR plan on an Internet site, compared to EMEA organisations (27%).
- And, more US organisations (32%) store the DR plan as a file on a laptop, compared to EMEA organisations (23%).



3.5 Which of the following people are on your organisation’s DR committee?



- Overall, 98% of organisations with a DR plan have a DR committee – only 2% do not.
- When it comes to DR committee membership, most commonly included are divisional / departmental IT managers (73%).

- Committee membership is also commonly given to other IT roles, such as systems / infrastructure manager (34%) and, more commonly, the CIO / CTO / IT director (55%).
- But 23% of organisations have their CEO as a member of the DR committee – but this means 77% do not.
- Also, 19% involve the CFO, 17% include other directors, 11% include the line of business heads, but fewer involve other non-IT senior managers (6%).
- Also, 17% include a chief security officer on their DR committee.
- Only 2% have external consultants on their DR committee.
- 71% of organisations involve 2 or more of these roles on the DR committee, whereas 46% involve 3 or more – but only 11% involve 5 or more and just 3% involve 7 or more [not shown].
- But 1 in 2 organisations (49%) only involve IT staff on the DR committee [not shown].
- Also, only 43% of organisations give DR committee membership to a mix of IT and non-IT staff [not shown].

"I have contacted the other business leaders and directors of the different departments. We discussed the company's requirements and created the plan together." Germany, IT Manager, 100,000 employees, automotive sector.

"Every year, the general manager needs to sign the contract agreement. Ultimately it is his decision, but different department heads are involved in the planning." Germany, IT Manager, 3,500 employees, manufacturing sector.

"It was all discussed with the CEO. But we have not agreed it all yet." Germany, IT Director, 700 employees, public sector.

"Once a year we have a meeting about disaster recovery plans with various directors." Italy, IT Manager, 3,000 employees, banking sector.

"IT security staff and other company directors agreed the plan." Russia, IT Director, 2,330 employees, power and energy sector.

"Just like in any other reputable organisation, the management, together with the heads of departments, were involved in the discussions about the DR plan. Data backup procedures are now part of the daily responsibilities of managers across departments. Heads of other departments were involved and agreement was reached." Russia, IT Director, 575 employees, public sector.

"We've done a detailed review with the business owners of each application so they understand the business requirements. (Researcher - Which directors have been involved, and what sort of threats have you discussed?) The Executive Board. (Researcher - And what sort of threats have you discussed?) All of the threats." UK, Head of IT, 160,000 employees, banking sector.

"We have discussed in great detail the potential threat to America and our organisation. I have spoken to the CEO and the Chairman about how we could protect the company." USA, IT Manager, 1,000 employees, investment banking sector.

"I have discussed with senior Board members the need for a disaster recovery plan, and this was successfully implemented in 2005." USA, IT Manager, 1,800 employees, investment banking sector.

"All the discussions about the DR plan mainly take place within the IT department. We are the ones who discuss all about the possible risks. But yes myself and the organisation's

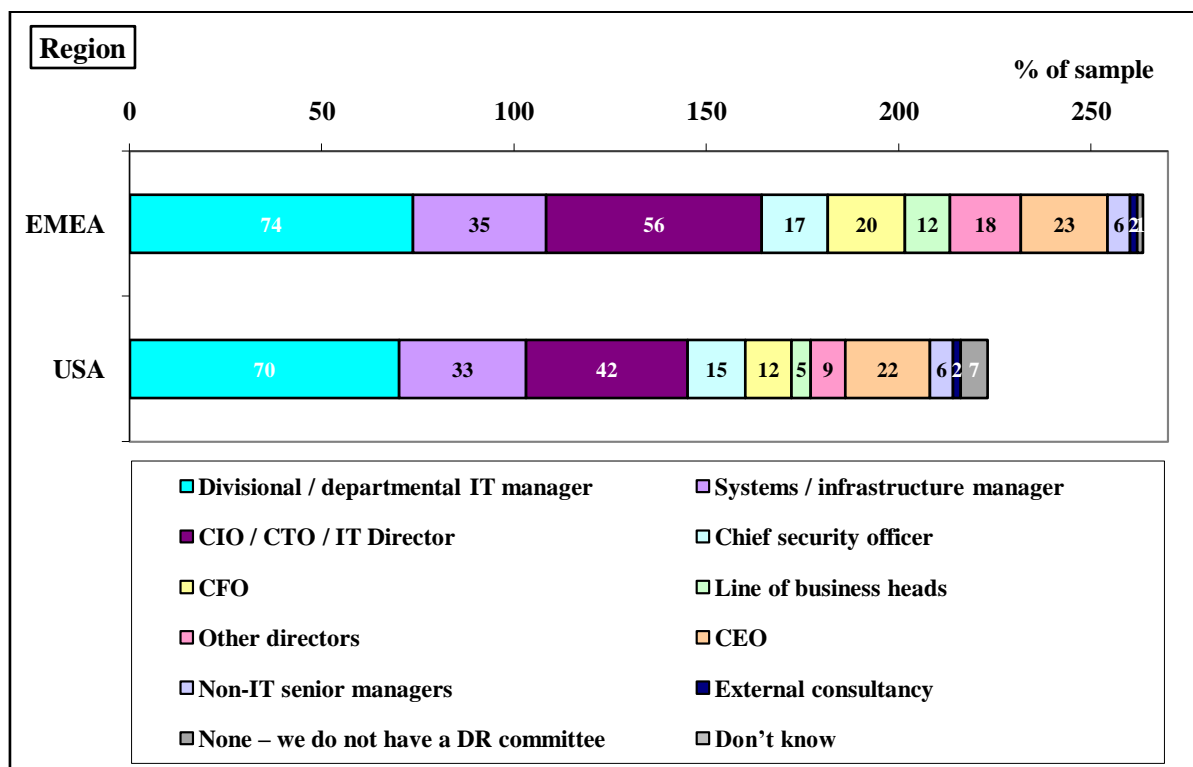
management agree it in the end.” Russia, IT Director, 3,000 employees, power and energy sector.

“I made the decisions myself. I have not agreed it with anyone.” Israel, IT Manager, 3,000 employees, public sector.

“I don't think it has been discussed with the directors. It's been discussed internally. (Researcher - In IT only?) Yes. We look at ourselves as service deliverers; there's not been input from business managers throughout the council. We just prioritise. (Researcher - Which directors have been involved, and what sort of threats have you discussed?) The threats are to email and payroll and we have been autonomous taking that decision. The plan was done internally within IT. (Researcher - Have you reached agreement?) Only in IT.” UK, IT Manager, 2,500 employees, public sector.

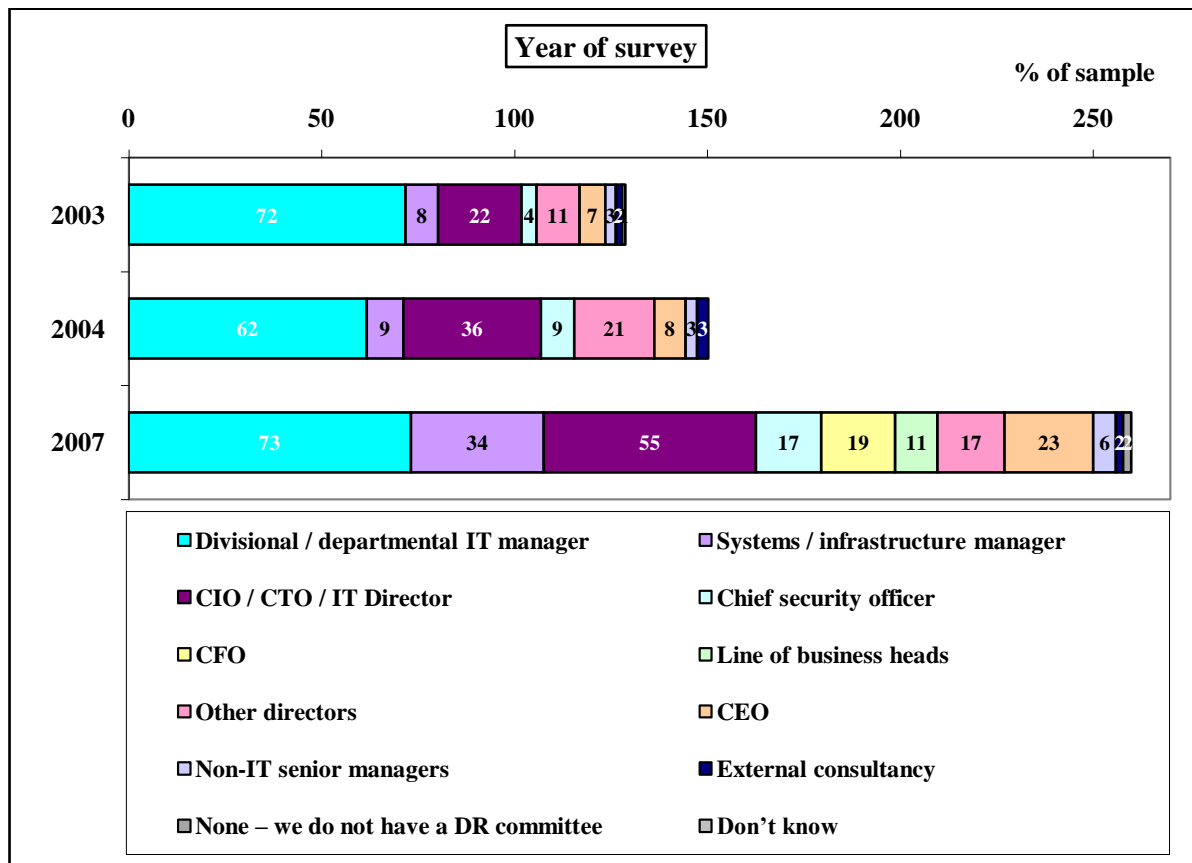
“I would say as part of the IT DR process, it's been limited; but we have a business continuity plan. (Researcher - So which business directors have you discussed it with?) No, none were involved. It was based on my understanding of their needs.” UK, IT Manager, 600 employees, public sector.

“I decided with my IT colleagues only.” USA, IT Manager, 900 employees, public sector.



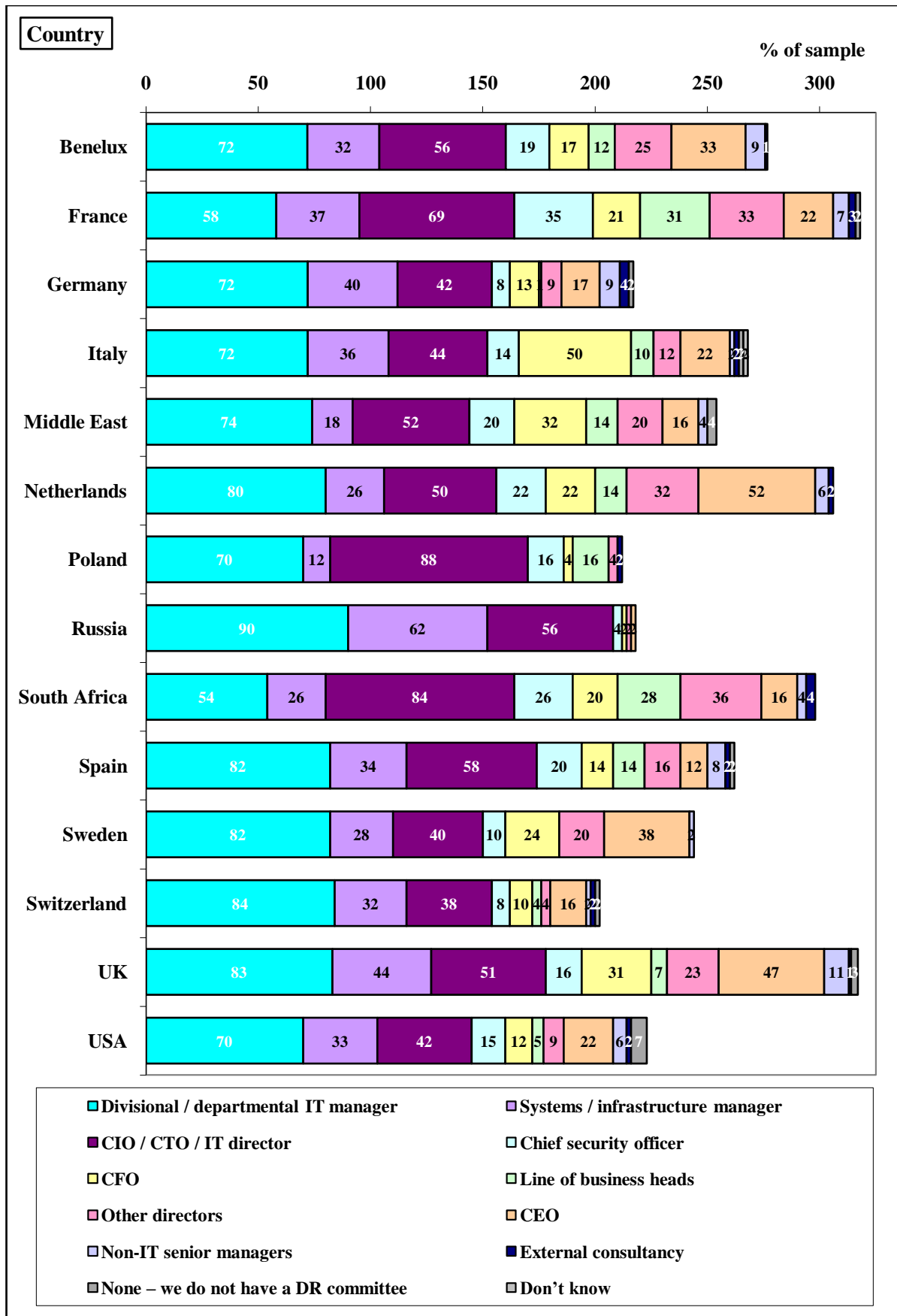
- More EMEA organisations (99%) have a DR committee, compared to US organisations (93%).
- And overall, EMEA organisations involve more of these people on their organisation's DR committee, compared to US organisations (i.e. length of bars in the above chart).
- Indeed, more EMEA organisations (72%) include 2 or more of these people on the DR committee, compared to US organisations (61%) [not shown].
- In detail, more EMEA organisations (56%) have the CIO / CTO / IT director on the DR committee, compared to US organisations (42%).

- And, more EMEA organisations (12%) include the line of business heads, compared to US organisations (5%).
- Furthermore, more EMEA organisations (18%) include other directors, compared to US organisations (9%).

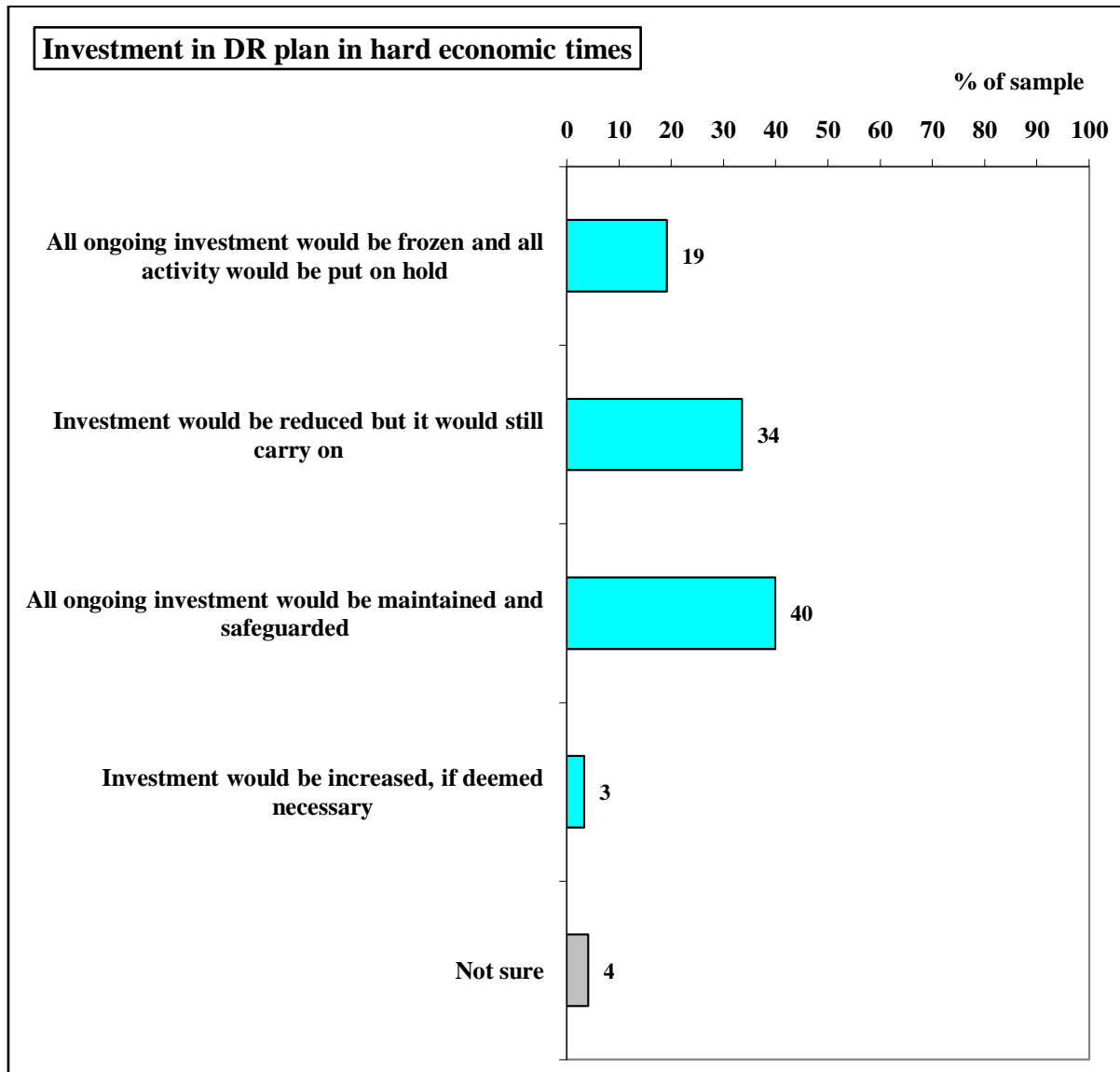


- More organisations questioned in 2003 (72%) and 2007 (73%) have divisional / departmental IT managers on the DR committee, compared to organisations questioned in 2004 (62%).
- But, more organisations questioned in 2007 (34%) have systems / infrastructure managers on the DR committee, compared to organisations questioned in 2003 (8%) and 2004 (9%).
- And, more organisations questioned in 2007 (55%) say the CIO / CTO / IT director is on the DR committee, compared to organisations questioned in 2003 (22%) and 2004 (36%).
- In addition, more organisations questioned in 2007 (17%) include a chief security officer on the DR committee, compared to organisations questioned in 2003 (4%) and 2004 (9%).
- Whereas, more organisations questioned in 2004 (21%) and 2007 (17%) have other directors on the DR committee, compared to organisations questioned in 2003 (11%).
- Yet, more organisations questioned in 2007 (23%) have the CEO on the DR committee, compared to organisations questioned in 2003 (7%) and 2004 (8%).

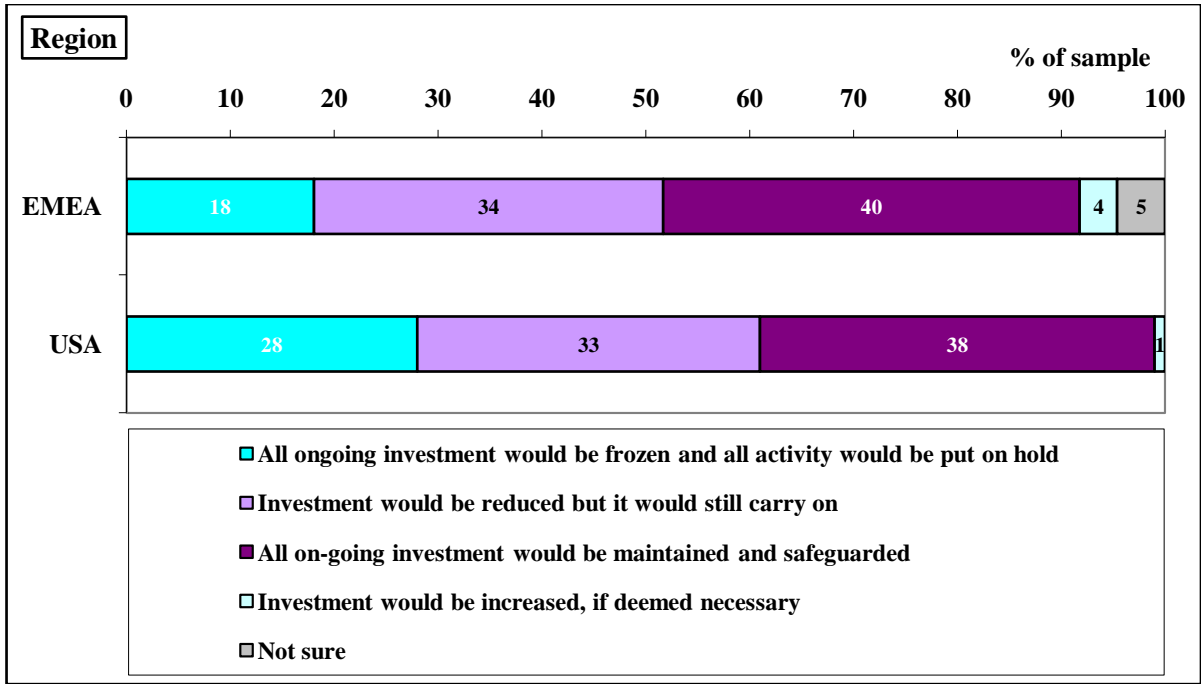
- And, more organisations questioned in 2007 (6%) include other non-IT senior managers on the DR committee, compared to organisations questioned in 2003 and 2004 (both 3%).
- More organisations questioned in 2003 (75%) and 2004 (64%) only involve IT staff on the DR committee, compared to 2007 (49%) [not shown].
- Similarly, more organisations questioned in 2007 (43%) give DR committee membership to a mix of IT and non-IT staff, compared to 2003 (11%) and 2004 (25%) [not shown].



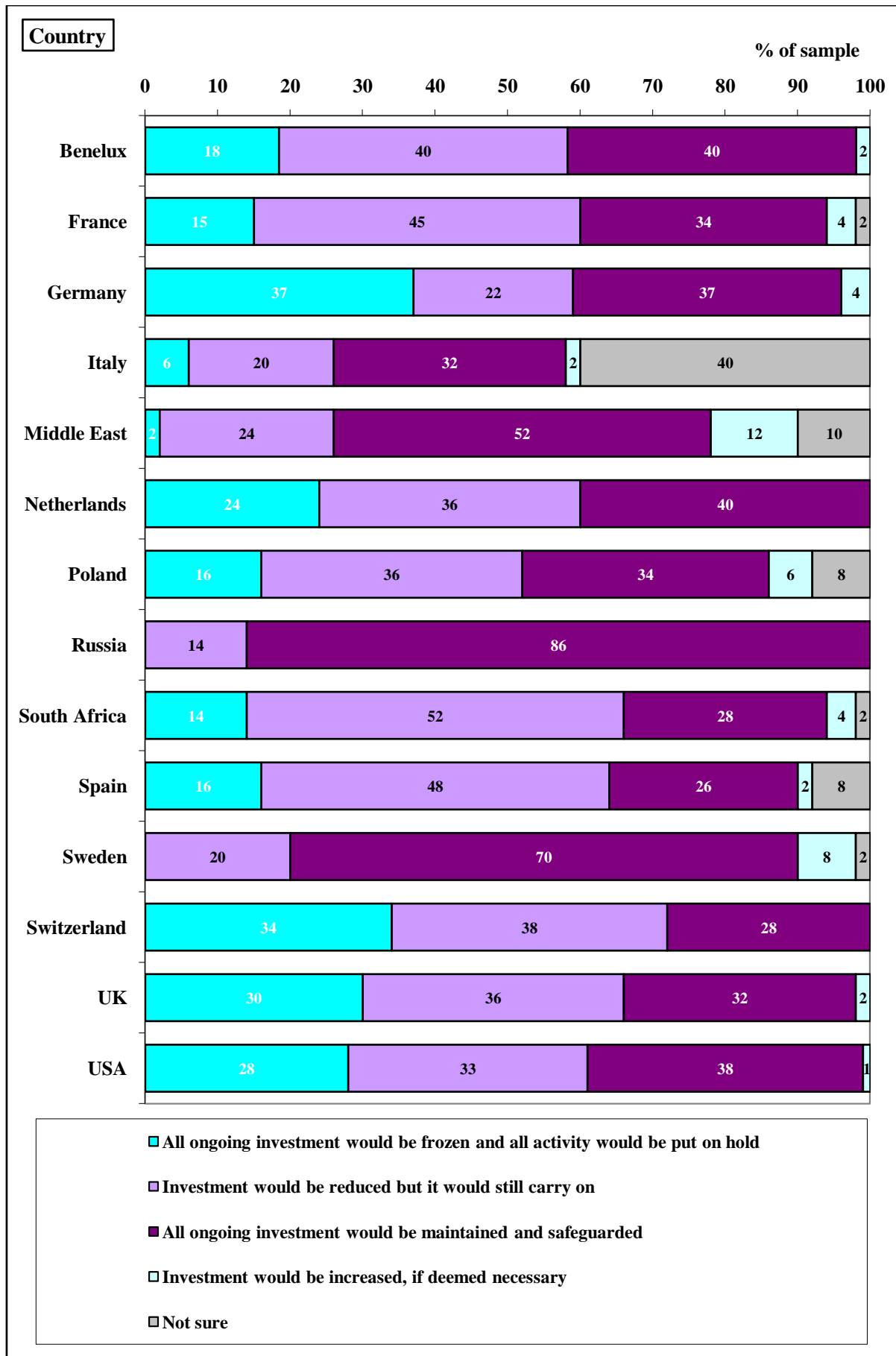
3.6 If your organisation were to fall on hard economic times tomorrow, which of the following would apply to the investment in your organisation’s DR plan?



- 19% of organisations say that if their organisation were to fall on hard economic times tomorrow, the investment in DR would be frozen and all activity would be put on hold.
- More (34%) say investment would be reduced, but it would still carry on if the organisation were to fall on hard economic times tomorrow.
- However, the largest group (40%) say all ongoing investment would be maintained and safeguarded.
- But only 3% say investment would be increased in hard economic times, if deemed necessary.
- Just 4% are not sure what would happen to the IT investment in DR if hard economic times were to strike.



- More US organisations (28%) say that if their organisation were to fall on hard economic times tomorrow, the investment in DR would be frozen and all activity would be put on hold, compared to EMEA organisations (18%).
- But, more EMEA organisations (5%) are not sure what would happen to the IT investment in DR if hard economic times were to strike, compared to US organisations (zero).



3.7 Which of the following technology types do you have and which are covered by the DR plan?

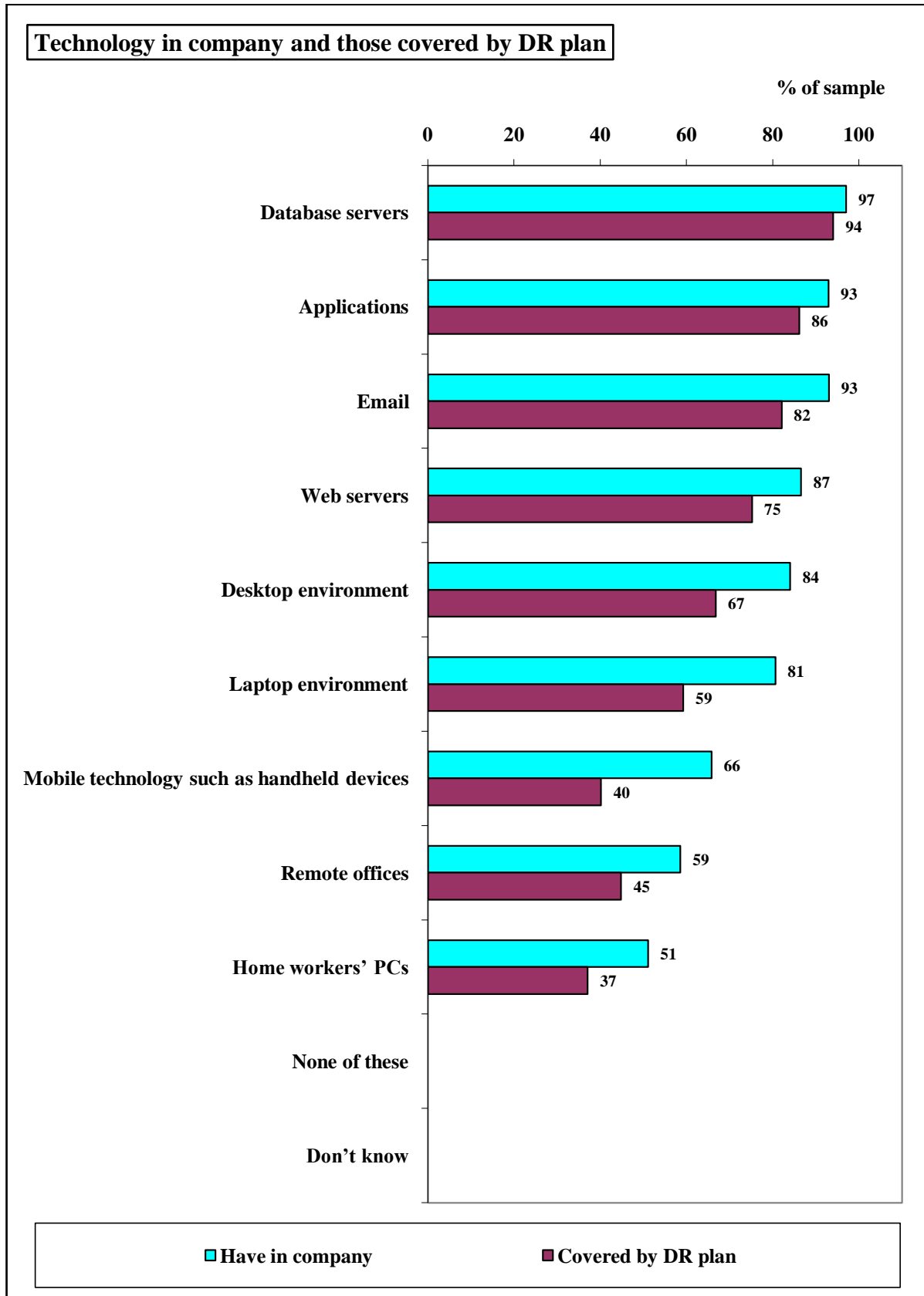
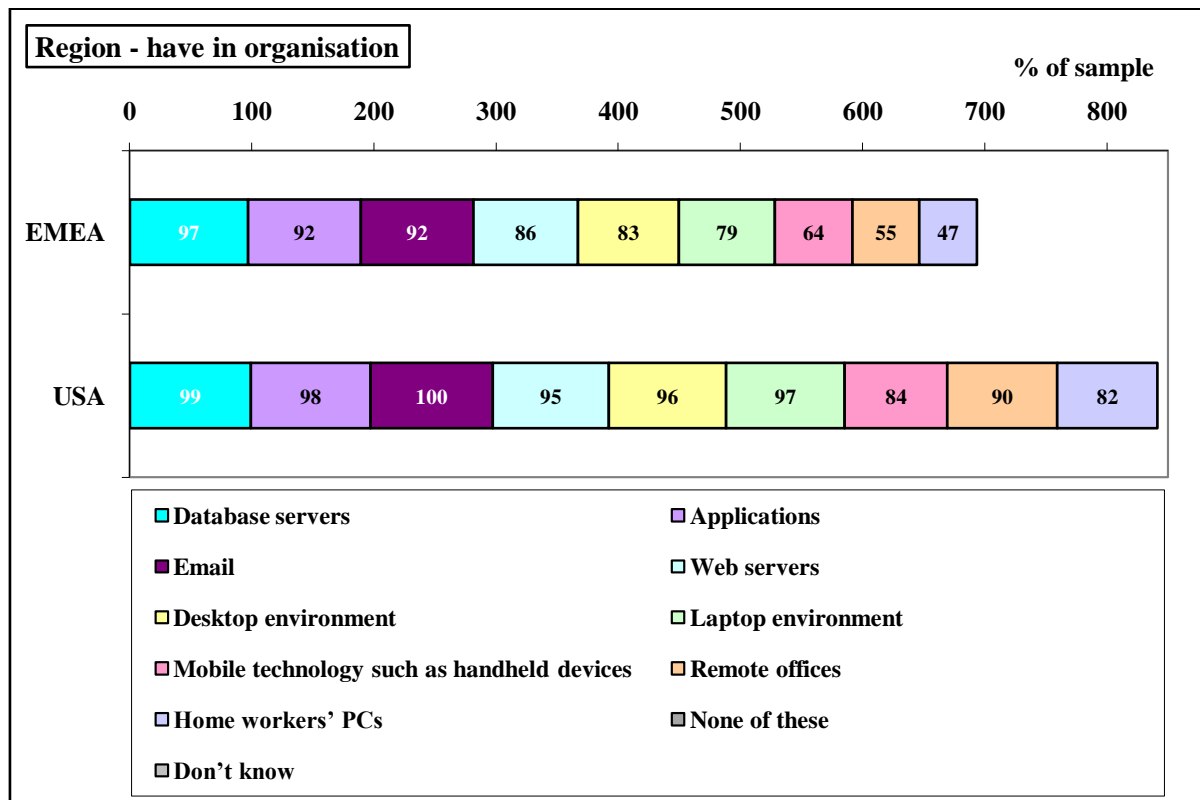


Table 8: Technology areas covered by the DR plan: whole sample

Areas of technology:	% of those that have technology in the organisation <u>and</u> have it covered by the DR plan:
Database servers	97%
Applications	93%
Email	88%
Web servers	87%
Desktop environment	79%
Laptop environment	73%
Mobile technology such as handheld devices	61%
Remote offices	77%
Home workers' PCs	73%

- Most DR plans cover database servers, applications, email and web servers, where they exist within an organisation.
- But fewer include the desktop environment, the laptop environment, remote offices and home workers' PCs.
- The least included area is mobile technology such as handheld devices.



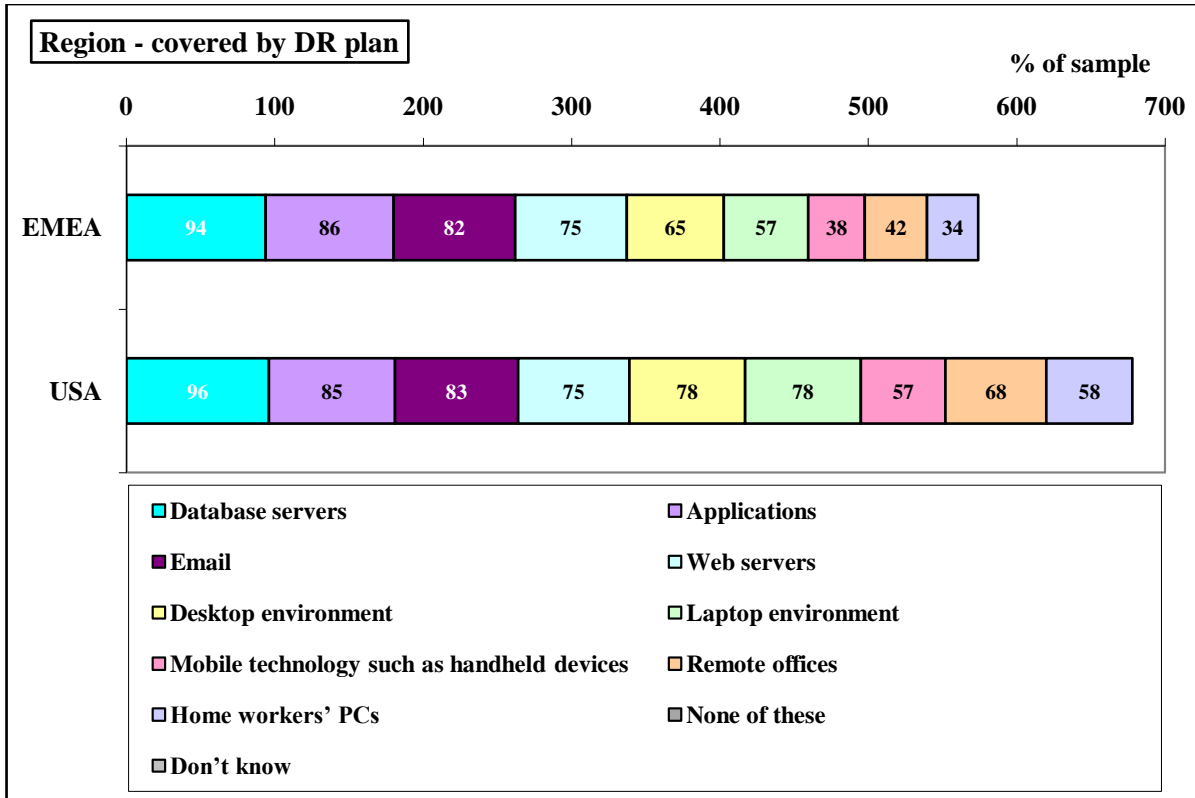


Table 9: Technology areas covered by the DR plan: regions

Areas of technology:	% of those that have technology in the organisation <u>and</u> have it covered by the DR plan:	
	EMEA	USA
Database servers	97%	97%
Applications	94%	87%
Email	89%	83%
Web servers	88%	79%
Desktop environment	79%	81%
Laptop environment	72%	80%
Mobile technology such as handheld devices	60%	68%
Remote offices	77%	76%
Home workers' PCs	73%	71%

- More EMEA organisations (94%) that have applications in the organisation cover them in their DR plan, compared to US organisations (87%).
- And, more EMEA organisations (88%) that have web servers in the organisation cover them in their DR plan, compared to US organisations (79%).

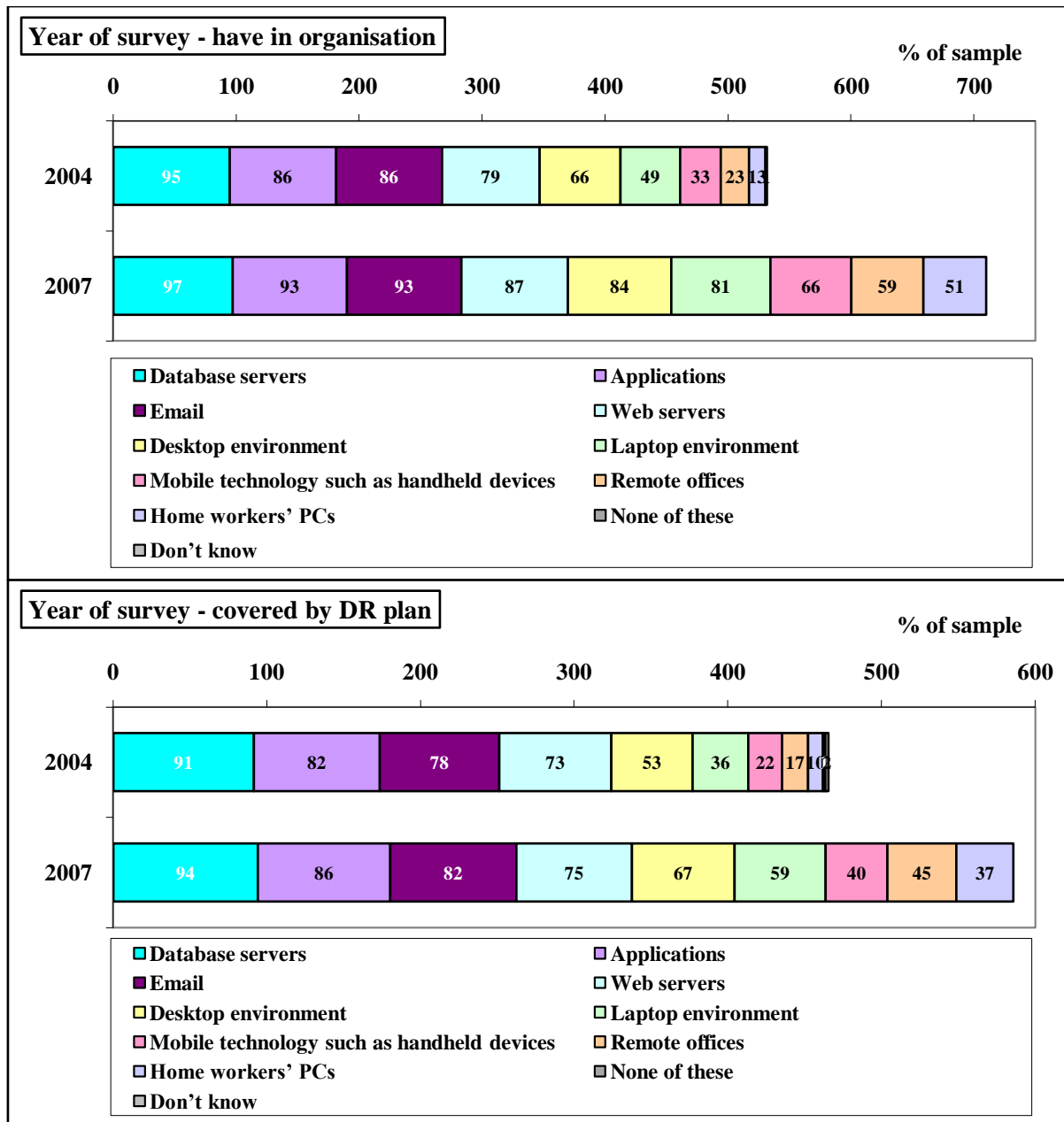
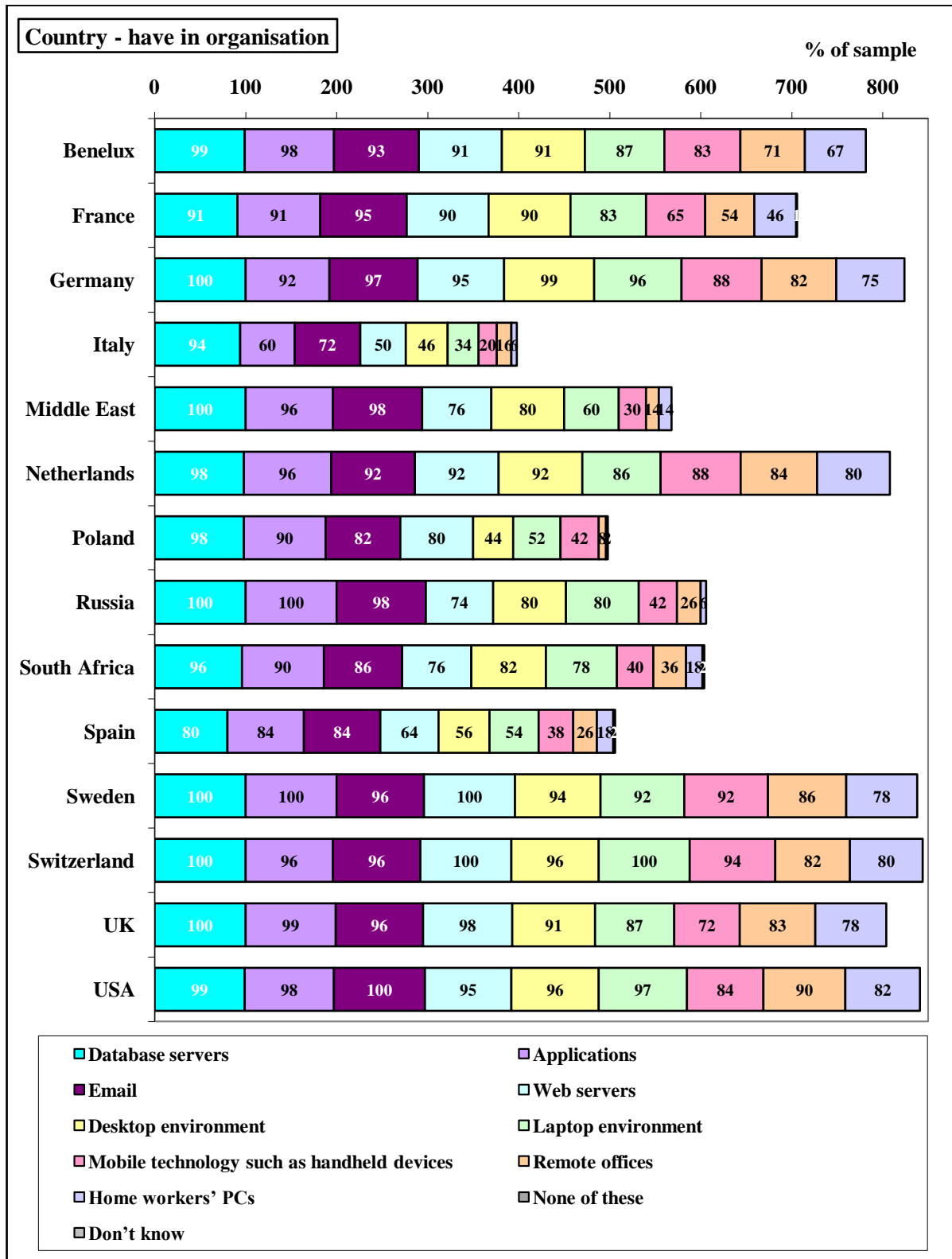


Table 10: Technology areas covered by the DR plan: year of survey

Areas of technology:	% of those that have technology in the organisation <u>and</u> have it covered by the DR plan:	
	2004	2007
Database servers	98%	97%
Applications	95%	93%
Email	90%	88%
Web servers	92%	87%
Desktop environment	81%	79%
Laptop environment	75%	74%
Mobile technology such as handheld devices	67%	61%
Remote offices	74%	77%
Home workers' PCs	66%	73%

- More organisations questioned in 2004 (92%) that have web servers in the organisation cover them in their DR plan, compared to 2007 (87%).



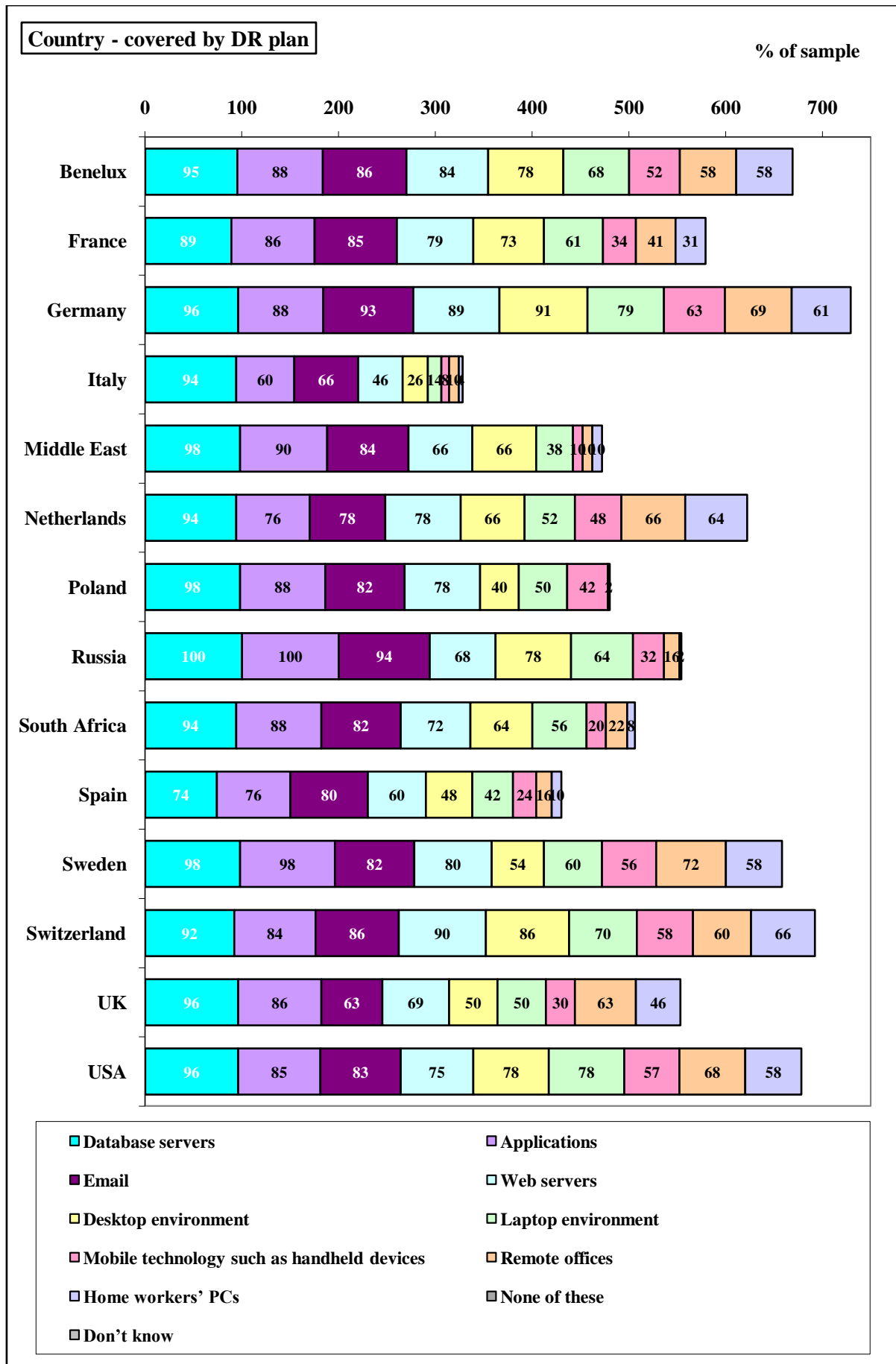
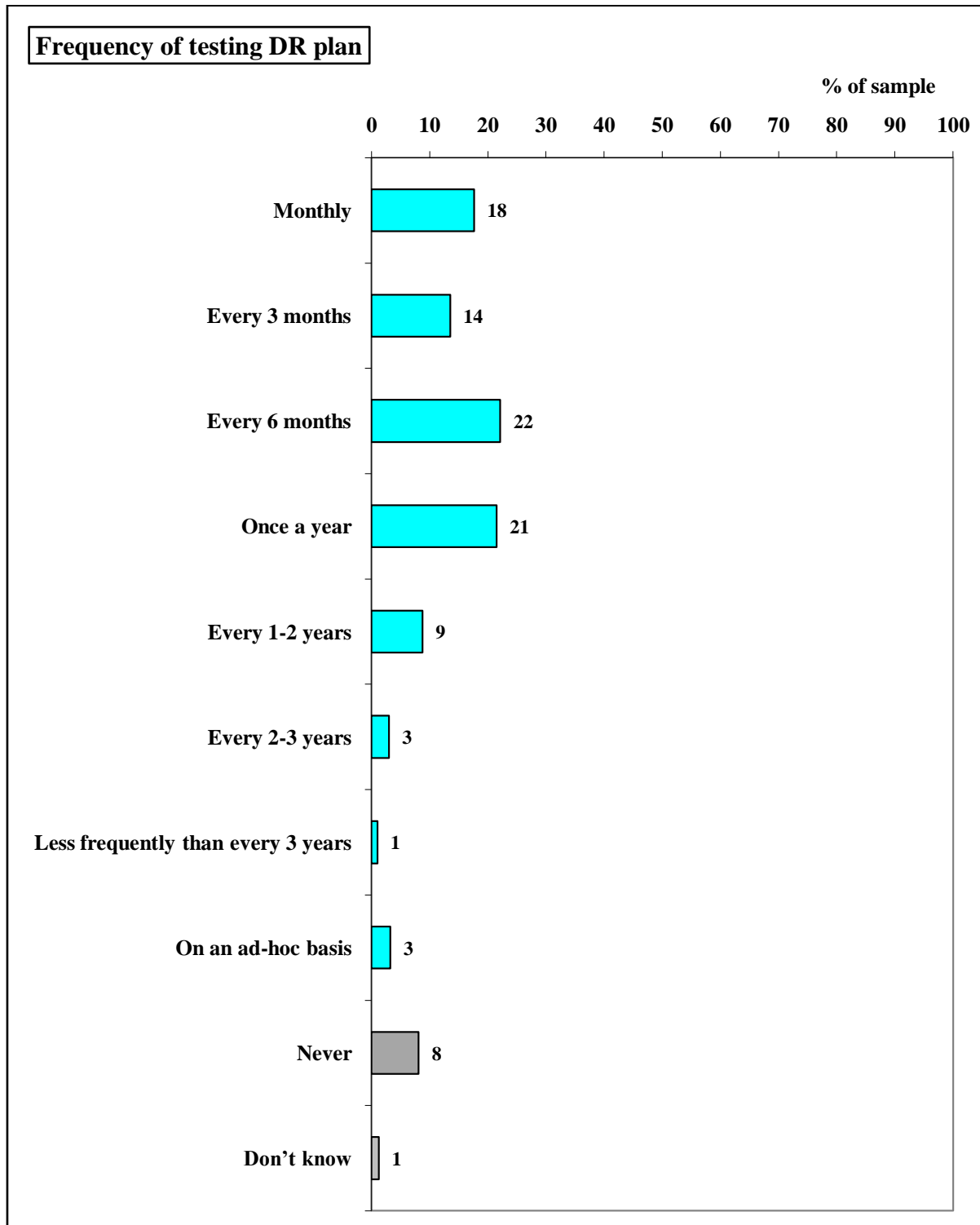


Table 11: Present technology covered by the DR plan: countries

Areas of technology:	% of those that have technology in the organisation <u>and</u> have it covered by the DR plan:													
	Benelux	France	Germany	Italy	Middle East	Nether lands	Poland	Russia	South Africa	Spain	Sweden	Switzerland	UK	USA
Database servers	96%	98%	96%	100%	98%	96%	100%	100%	98%	93%	98%	92%	96%	97%
Applications	90%	95%	96%	100%	94%	79%	98%	100%	98%	90%	98%	88%	87%	87%
Email	93%	89%	96%	92%	86%	85%	100%	96%	95%	95%	85%	90%	66%	83%
Web servers	93%	88%	94%	92%	87%	85%	98%	92%	95%	94%	80%	90%	70%	79%
Desktop environment	85%	81%	92%	57%	83%	72%	91%	98%	78%	86%	57%	90%	55%	81%
Laptop environment	78%	73%	82%	41%	63%	60%	96%	80%	72%	78%	65%	70%	57%	80%
Mobile technology such as handheld devices	63%	52%	72%	40%	33%	55%	100%	76%	50%	63%	61%	62%	42%	68%
Remote offices	82%	76%	84%	63%	71%	79%	25%	62%	61%	62%	84%	73%	76%	76%
Home workers' PCs	87%	67%	81%	67%	71%	80%	0%	33%	44%	56%	74%	83%	59%	71%

3.8 How frequently does your organisation carry out full scenario testing of its disaster recovery plan, involving relevant people, processes and technologies?



- Collectively, 91% of organisations carry out full scenario testing on their DR plans involving relevant people, processes and technologies.
- On average, however, this is once every 8 months [not shown].

- Just over half of the sample (54%) test more frequently than annually - 18% test monthly; 14% test every 3 months and 22% test every 6 months.
- Another 21% carry out such testing annually, but 13% test less frequently than annually, meaning, collectively, 34% carry out such tests annually or less frequently than this.
- Another 3% carry out full scenario tests on an ad-hoc basis.
- Only 8% do not carry out any full scenario testing and another 1% are unsure how frequently such testing is carried out, if at all.

"Every 6 months. (Researcher - Why?) Because we need to check reliability of the process so we can sleep well at night!" Israel, IT Manager, 3,000 employees, public sector.

"We carry out the full scenario testing twice a year in May and November. (Researcher - Why?) Because it's very demanding and it's an order from the Bank of Italy." Italy, IT Manager, 3,000 employees, banking sector.

"We do full testing every 9-10 months when we are closed. (Researcher - Why?) Because we can't do it while we are open. It is too disruptive." Saudi, IT Manager, 1,000 employees, public sector.

"Only once a year. (Researcher - Why?) Because we don't have time to do it." Germany, IT Manager, 800 employees, public sector.

"A minimum of once a year. (Researcher - Why?) We do various tests throughout the year. When we plan the test, sometimes operational requirements delay it." UK, IT Manager, 500 employees, telecoms sector.

"We aim to carry it out once a year. We try to carry this out a month or two before potential floods could occur." USA, IT Manager, 1,800 employees, investment banking sector.

"We have not yet had a full scenario test. (Researcher - Why?) Departments like to manage their own data, and the test helps employees to appreciate how the plan is working, but testing has been piecemeal." Russia, IT Director, 510 employees, public sector.

"We would not do so at all. We have taken email servers out yesterday though. (Researcher - Why can't you do it?) Because it would involve taking out a building. But we take routers out and the backup kicks in, so we don't even notice. Even if the primary link goes down, we are still okay. We did an email test yesterday which admittedly we did at 5.30pm after working hours." UK, IT Manager, 2,500 employees, public sector.

"Backup is every hour, but scenarios are rarely tested." Germany, IT Manager, 100,000 employees, automotive sector.

"Never. (Researcher - Why?) It takes a long time and is very costly." Germany, IT Manager, 2,500 employees, public sector.

"We never carry out full scenario testing." USA, IT Manager, 1,000 employees, investment banking sector.

"Never. (Researcher - Why?) Because it takes a lot of time." USA, IT Manager, 3,500 employees, public sector.

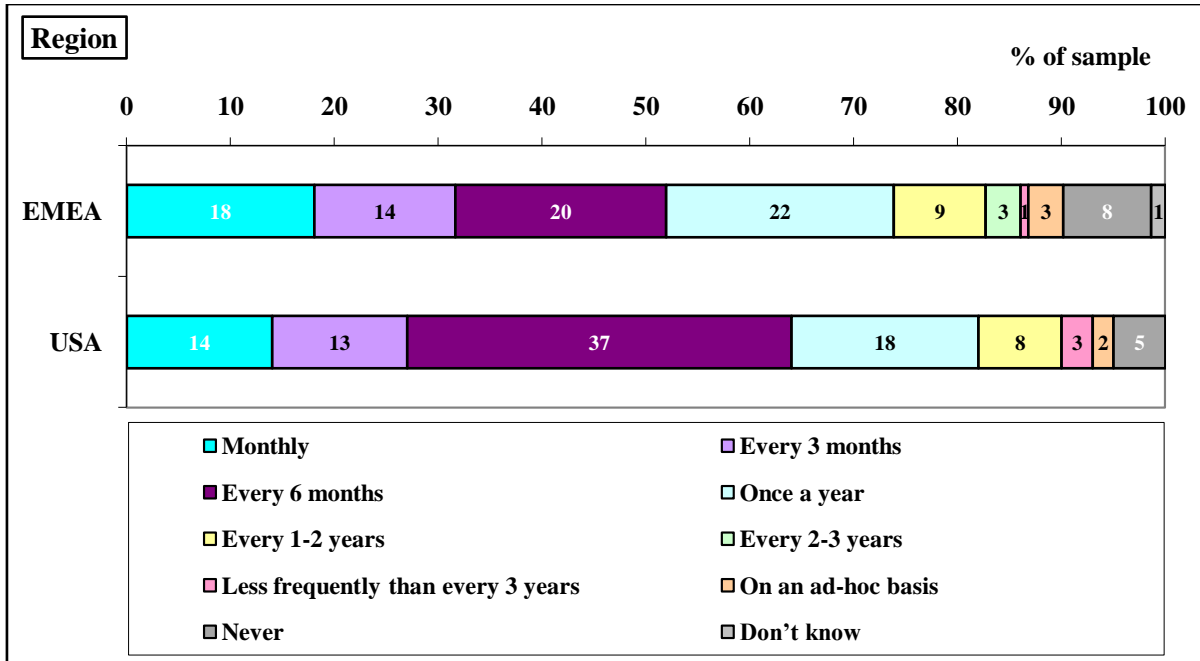


Table 12: Average frequency of testing: regions

Region	Average frequency
EMEA	7.8 months
USA	8.1 months

- More US organisations (37%) carry out full scenario testing every 6 months, compared to EMEA organisations (20%).
- But, on average, there is no difference according to region and how frequently organisations run full scenario tests of their DR plan.

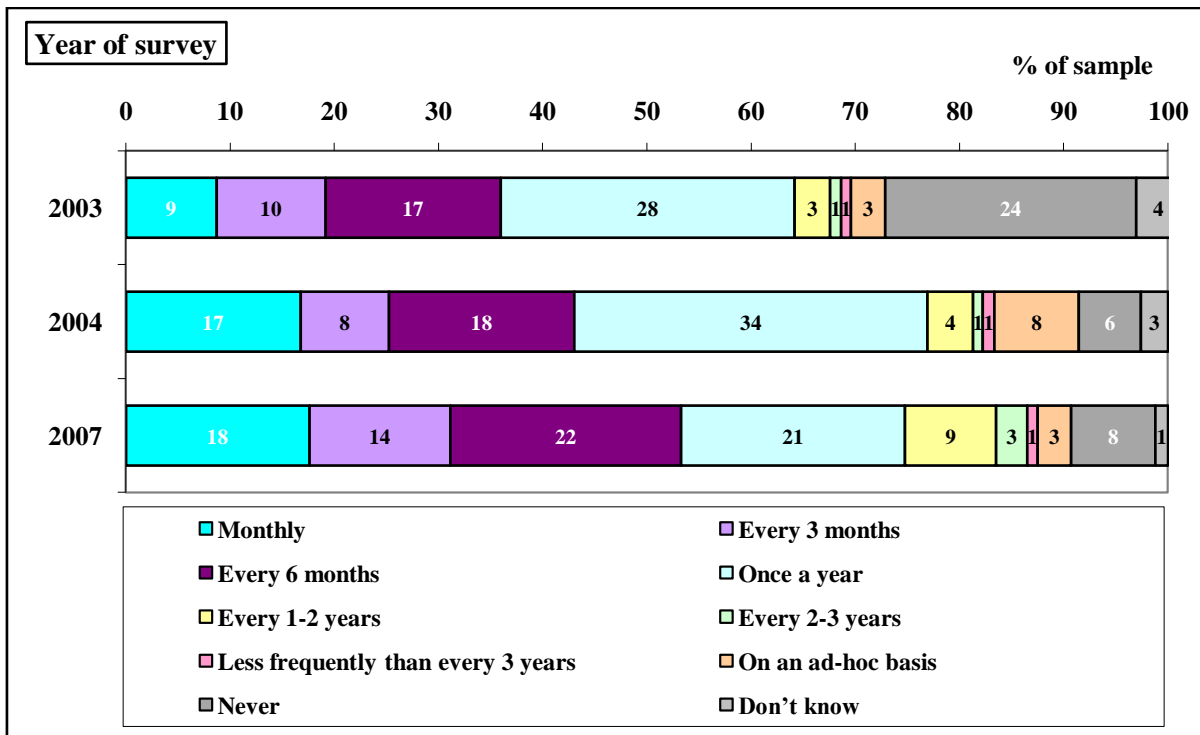


Table 13: Average frequency of testing: year of survey

Year of survey	Average frequency
2003	6.7 months
2004	8.1 months
2007	7.8 months

- More organisations questioned in 2004 (17%) and 2007 (18%) carry out full scenario testing on their DR plans involving relevant people, processes and technologies on a monthly basis, compared to organisations questioned in 2003 (9%).
- But, more organisations questioned in 2007 (14%) carry out full scenario testing on their DR plans every 3 months, compared to 2003 (10%) and 2004 (8%).
- Yet, more organisations questioned in 2007 (22%) carry out full scenario testing on their DR plans every 6 months, compared to 2003 (17%) and 2004 (18%).
- However, more organisations questioned in 2003 (28%) and 2004 (34%) carry out full scenario testing on their DR plans once a year, compared to 2007 (21%).
- But, more organisations questioned in 2007 (9%) carry out full scenario testing on their DR plans every 1 to 2 years, compared to 2003 (3%) and 2004 (4%).
- More organisations questioned in 2004 (8%) carry out full scenario testing on their DR plans on an ad-hoc basis, compared to 2003 and 2007 (both 3%).
- Finally, more organisations questioned in 2003 (24%) never carry out full scenario testing on their DR plans, compared to 2004 (6%) and 2007 (8%).

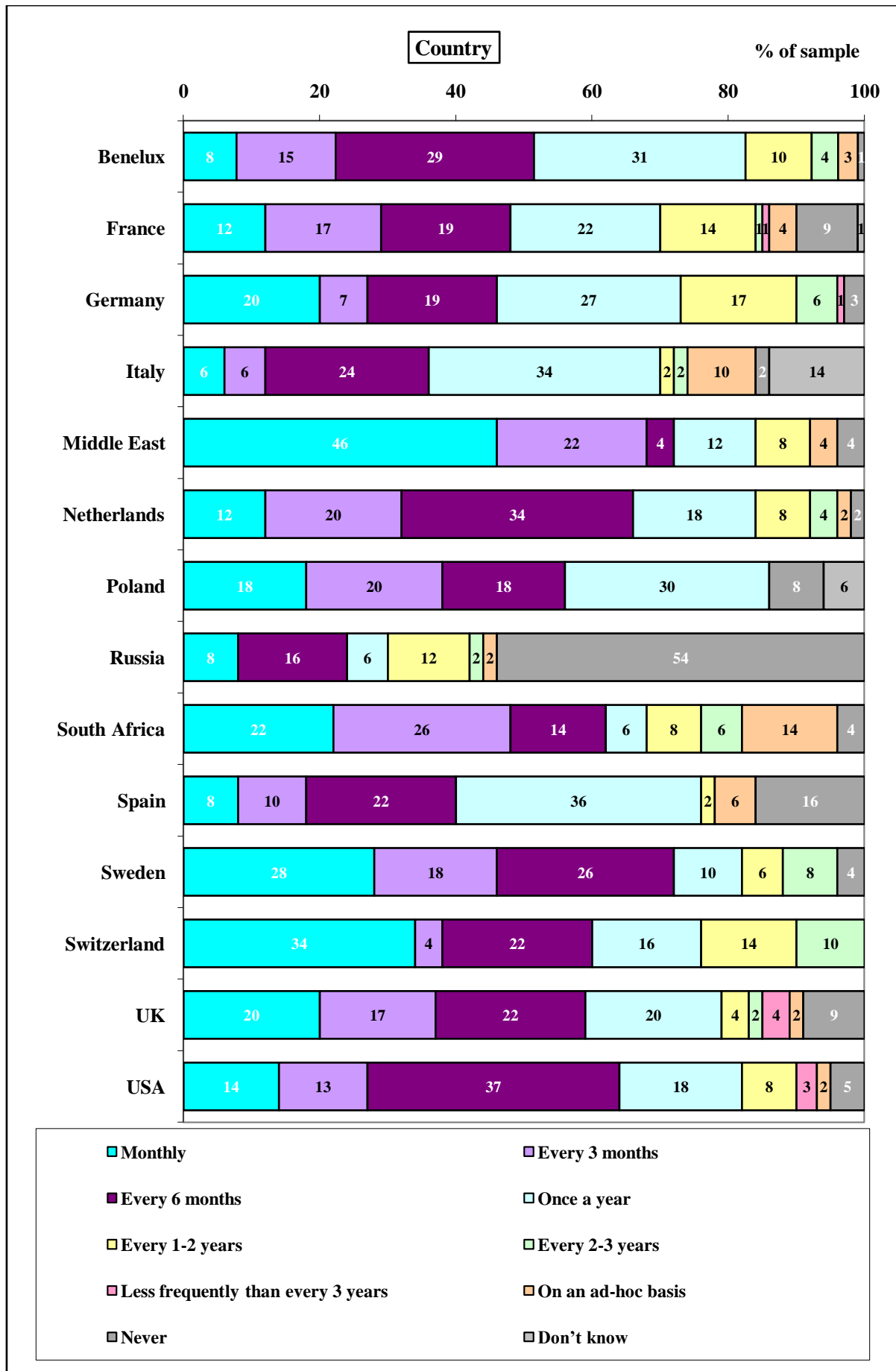
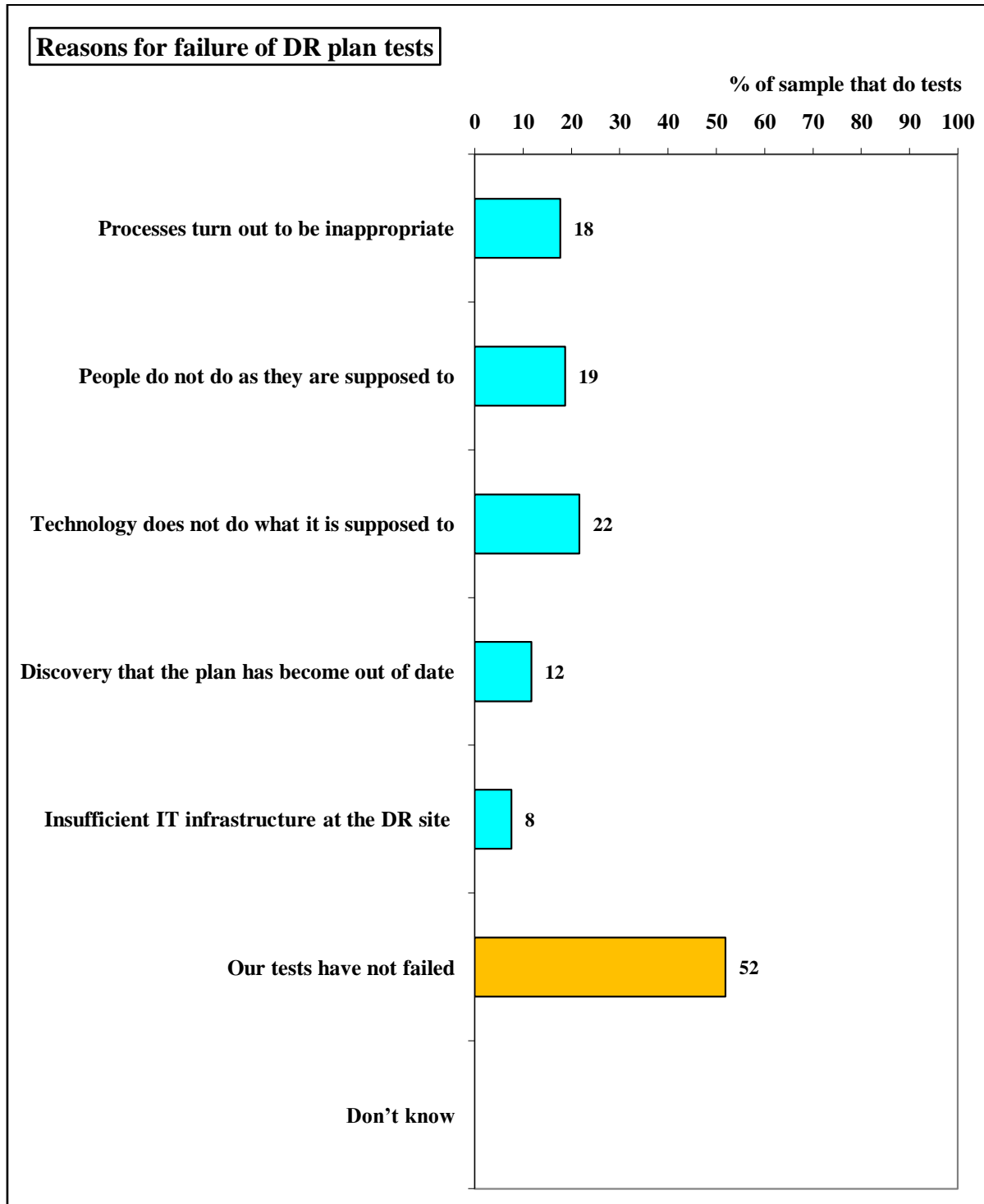


Table 14: Average frequency of testing: countries

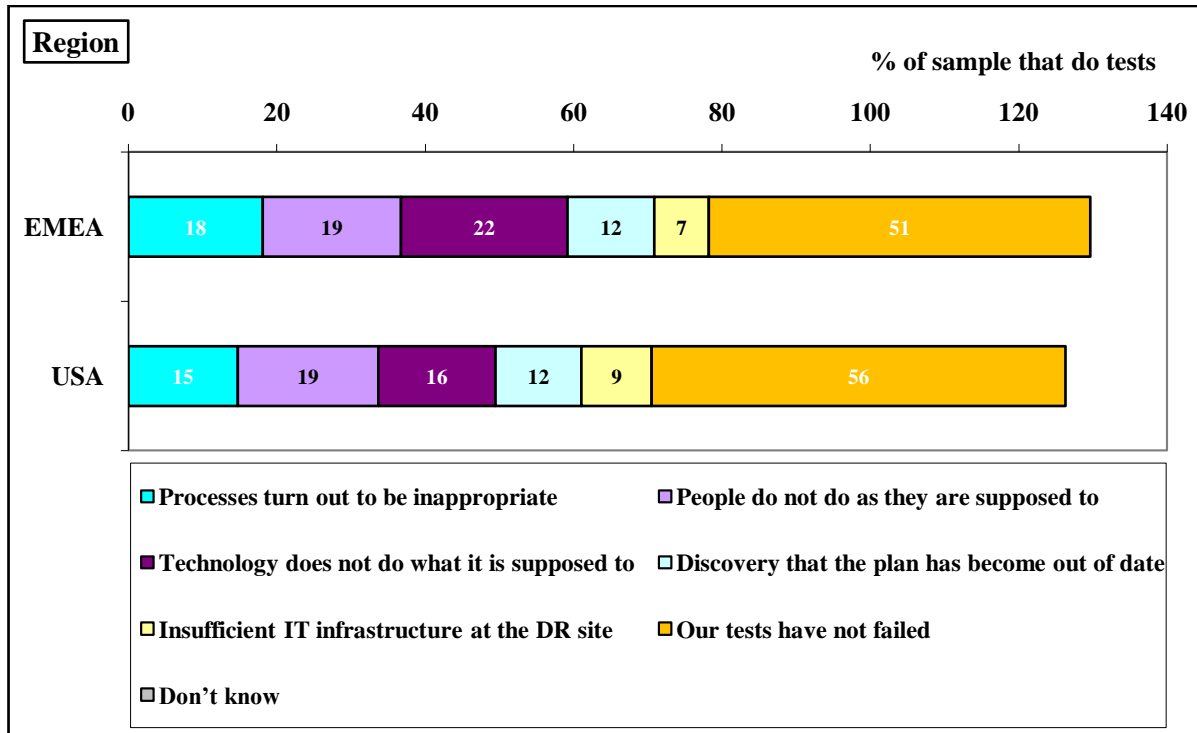
Countries	Average frequency
Benelux	9.2 months
France	8.2 months
Germany	10.2 months
Italy	8.8 months
Middle East	4.4 months
Netherlands	7.7 months
Poland	5.8 months
Russia	4.6 months
South Africa	6.7 months
Spain	6.8 months
Sweden	7.1 months
Switzerland	9.2 months
UK	8.1 months
USA	8.1 months

3.9 [Just to those that do tests] Which of the following reasons accounts for why full scenario tests have failed?

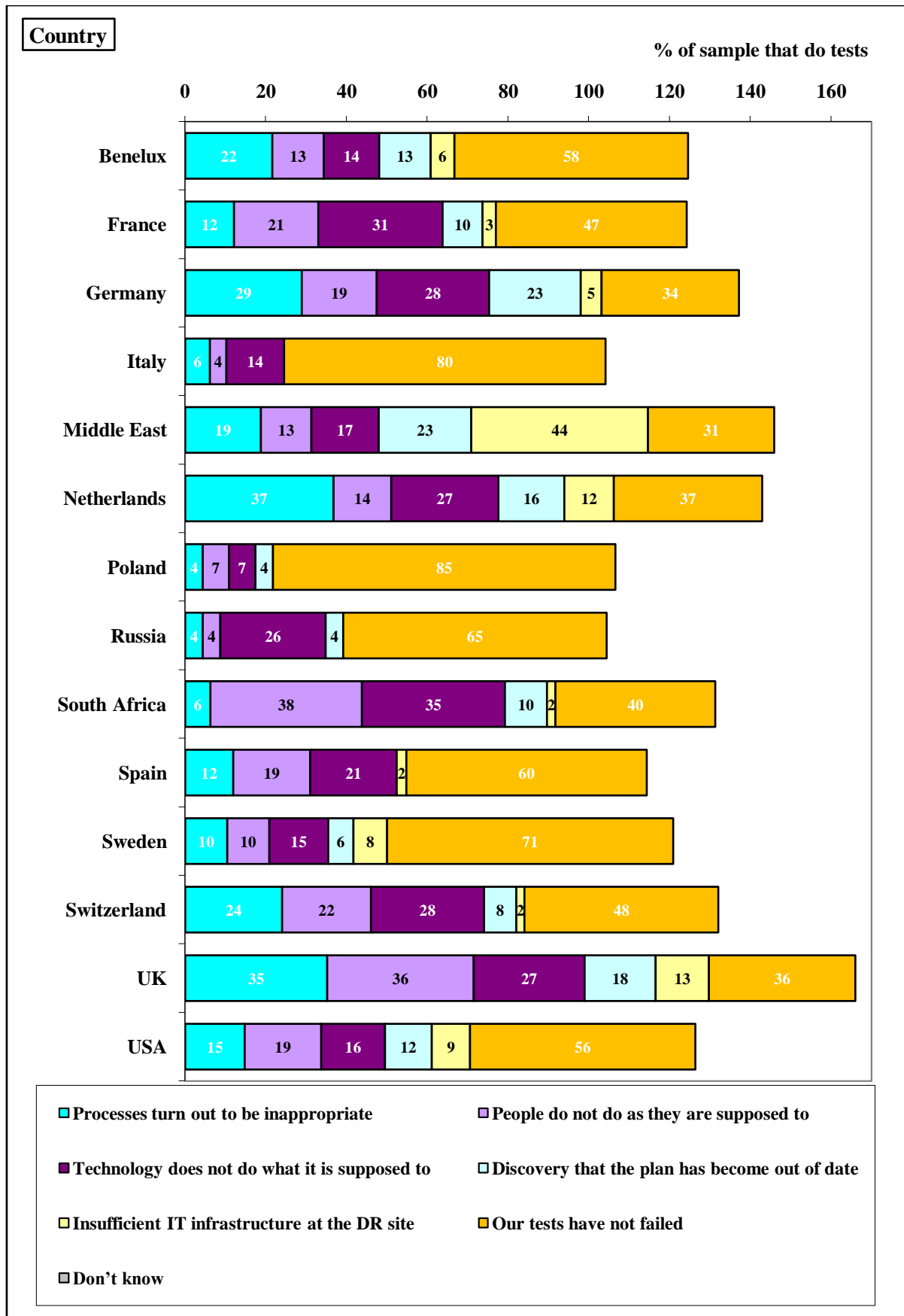


- Collectively, 48% of those that carry out full scenario tests say they have failed.
- The main reason for DR test failure is that the technology does not do what it is supposed to (22%).
- This is followed very closely by 19% of organisations that say people do not do what they are supposed to.

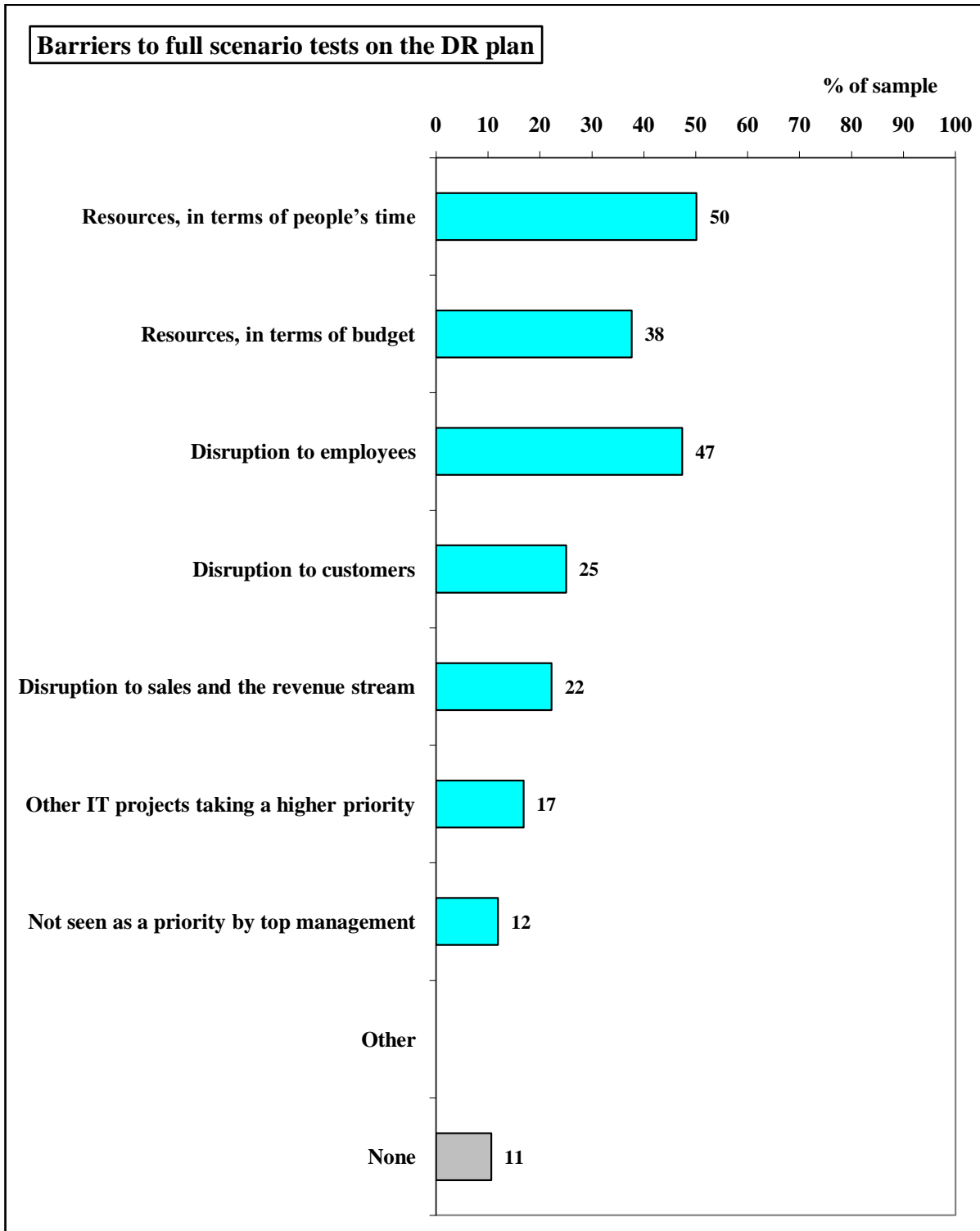
- But almost as many (18%) say the DR processes turn out to be inappropriate.
- 12% say tests fail as they discover their DR plan has become out of date.
- Only 8% of organisations say the DR full scenario tests have failed due to insufficient IT infrastructure at the DR site.
- 21% say their tests have failed for more than 1 reason, and 7% say 3 of these reasons apply [not shown].
- In contrast, 52% say their DR tests have not failed.



- Statistically, there is no difference according to region and why full scenario tests of the DR plan have failed.



3.10 Which of the following do you consider to be barriers to running a full scenario test on your disaster recovery plan?



- Collectively, 89% of organisations think there are barriers to carrying out full scenario testing on their DR plans.
- Indeed, 67% say 2 or more of these barriers apply; and 37% think 3 or more are barriers for them [not shown].

- The Top 3 barriers are:
 1. Resources, in terms of people's time (50%)
 2. Disruption to employees (47%)
 3. Resources, in terms of budget (38%)
- 25% think that disruption to customers is a barrier to full scenario testing of their DR plan, and 22% say disruption to sales and the revenue stream is a barrier.
- However, 17% say other IT projects take a higher priority than full testing of the DR plan.
- But only 12% say full scenario DR testing is not seen as a priority by top management.
- In contrast, 11% say none of these present barriers to full scenario testing of their DR plan.

"Time is the main barrier and also having key people involved." Jordan, IT Manager, 4,000 employees, banking sector.

"Cost and the time. We need more or less 10 people on Saturday." Italy, IT Manager, 1,600 employees, banking sector.

"Time and resources." USA, IT Manager, 510 employees, public sector.

"The only barrier is the potential for lost productivity, but if we have an actual disaster the potential for lost productivity would have been greater by comparison. I force it through if I have to." UK, IT Manager, 670 employees, public sector.

"The day-to-day impact on the running of the business." UK, Head of IT, 160,000 employees, banking sector.

"Most likely the human element. We would need time to mobilise and convince people of the benefits of conducting this on a larger scale." Russia, IT Director, 510 employees, public sector.

"It needs at LEAST one hour to run and we can't have system downtime." Germany, IT Manager, 100,000 employees, automotive sector.

"The main barrier is time, because we need computers up and running 24 hours a day, 365 days a year." Germany, IT Manager, 800 employees, public sector.

"The internal organisation of employees and systems are the main barriers." Italy, IT Manager, 800 employees, banking sector.

"Costs. No one wants to take the responsibility of running a full test." Russia, IT Director, 3,450 employees, power and energy sector.

"Probably, ownership. Getting people involved and getting management on board." UK, IT Manager, 2,500 employees, public sector.

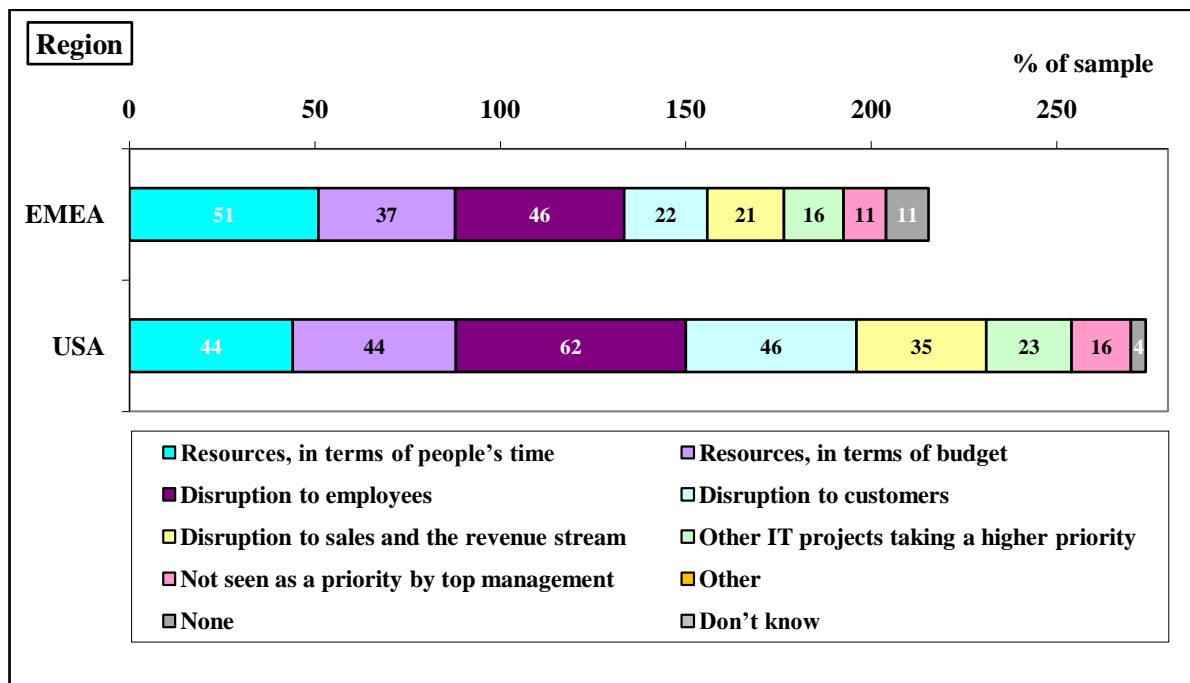
"Shortage of experienced specialists." Russia, IT Director, 2,330 employees, power and energy sector.

- There seems to be a false sense of security among those that have not yet tested their DR plan.

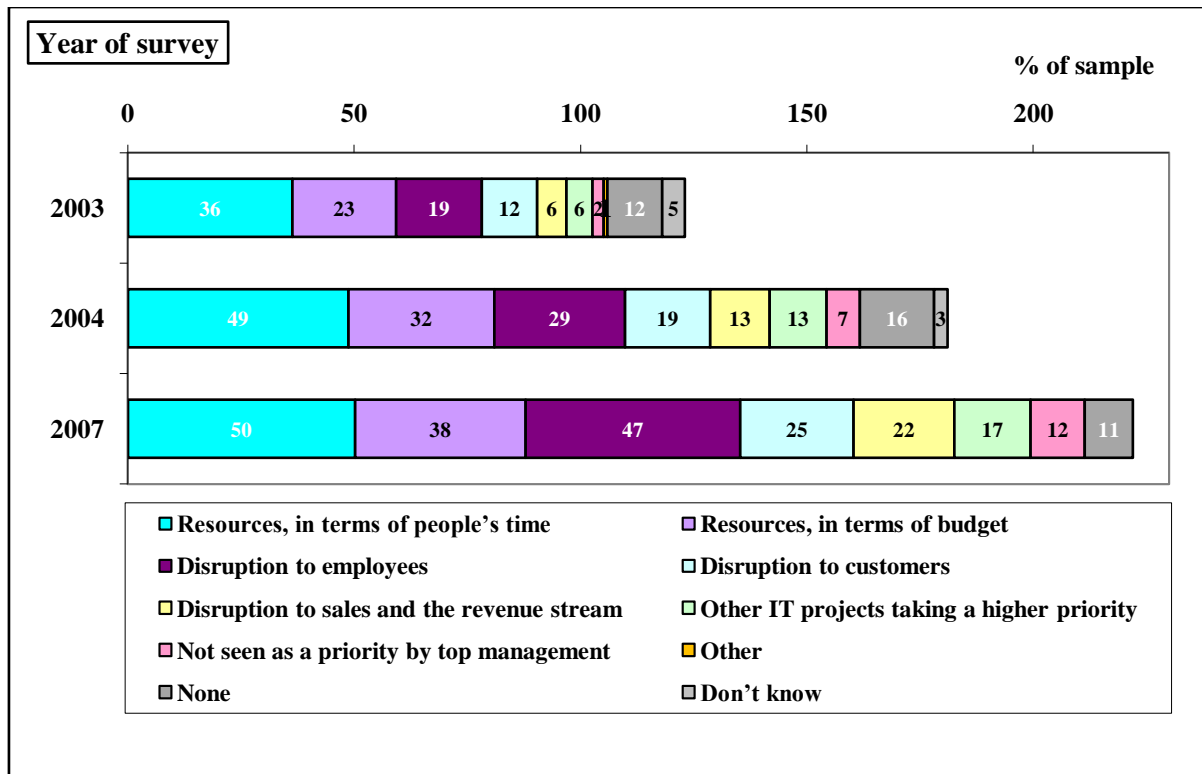
"We are sceptical about testing something unless we deem it fully necessary. If for some reason our plan didn't work, we would only like to discover this in the event of a disaster." USA, IT Manager, 1,000 employees, investment banking sector.

"I don't think we will have any barriers when we do it." Italy, IT Director, 550 employees, public sector.

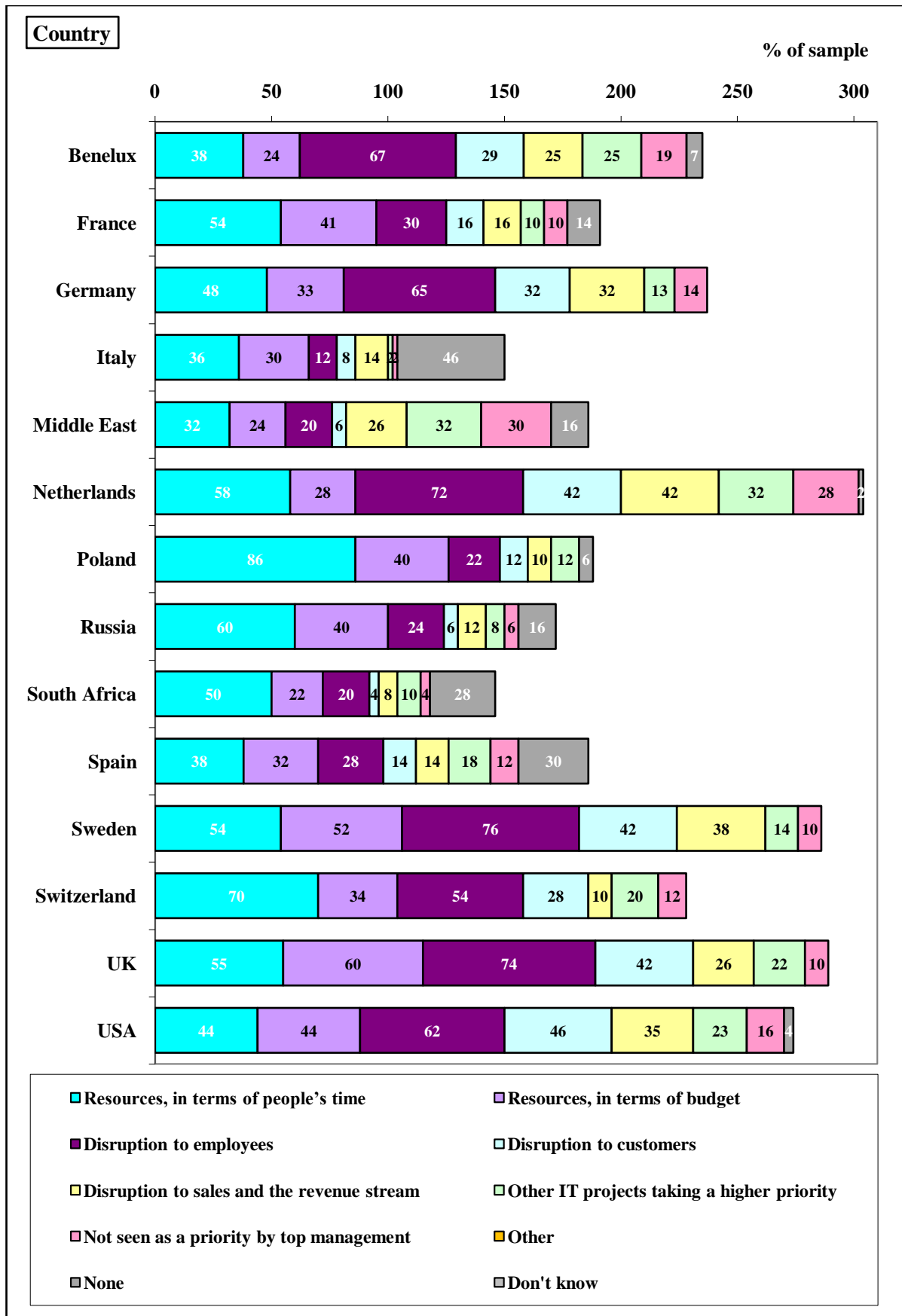
"I don't think there are any barriers; we just haven't done it." USA, IT Manager, 1,500 employees, local and federal government.



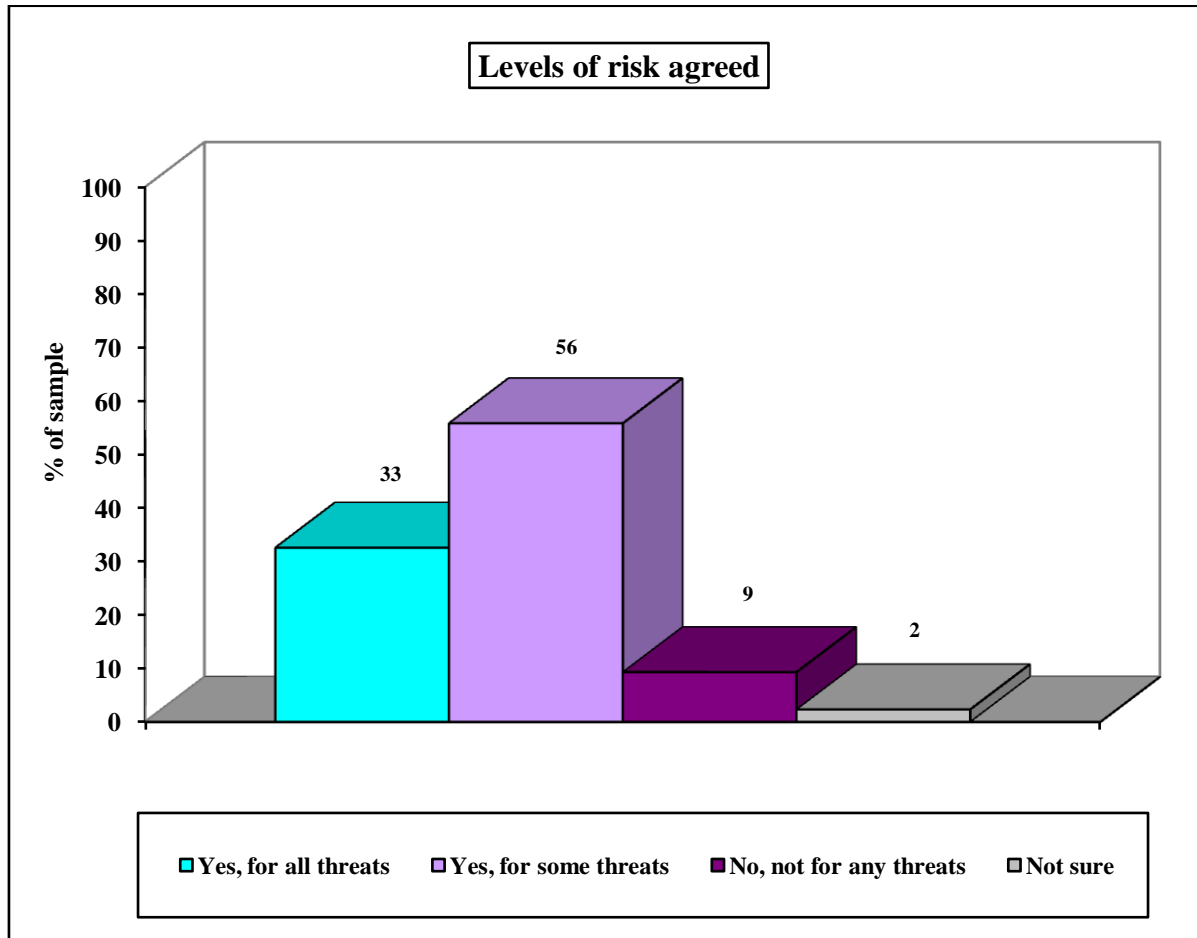
- Overall, US organisations say more of these barriers apply to their organisation's DR plan testing, compared to EMEA organisations (i.e. length of bars in the above chart).
- Indeed, more US organisations (96%) think at least 1 of these barriers applies to carrying out full scenario testing on their DR plans, compared to EMEA organisations (89%).
- And, more US organisations (79%) say 2 or more of these barriers apply, compared to EMEA organisations (66%) [not shown].
- Furthermore, more US organisations (59%) say 3 or more of these barriers apply, compared to EMEA organisations (34%) [not shown].
- In detail, more US organisations (62%) say disruption to employees is a barrier to testing, compared to EMEA organisations (46%).
- Also, more US organisations (46%) think disruption to customers is a barrier to testing, compared to EMEA organisations (22%).
- In addition, more US organisations (35%) say disruption to sales and the revenue stream is a barrier, compared to EMEA organisations (21%).
- But, more EMEA organisations (11%) say none of these present barriers to full scenario testing of their DR plan, compared to US organisations (4%).



- Overall, organisations questioned in 2007 say more of these barriers apply to their organisation's DR plan testing, compared to previous years (i.e. length of bars in the above chart)
- In detail, more organisations questioned in 2004 (49%) and 2007 (50%) think resources, in terms of people's time, is a barrier to full scenario testing of their DR plan, compared to organisations questioned in 2003 (36%).
- Also, more of those questioned in 2004 (32%) and 2007 (38%) think resources, in terms of budget, is a barrier, compared to 2003 (23%).
- But, more of those questioned in 2007 (47%) say that disruption to employees is a barrier, compared to 2003 (19%) and 2004 (29%).
- In addition, more of those questioned in 2007 (25%) say that disruption to customers is a barrier, compared to 2003 (12%) and 2004 (19%).
- And, more of those questioned in 2007 (22%) say disruption to sales and the revenue stream is a barrier, compared to 2003 (6%) and 2004 (13%).
- Yet, more of those questioned in 2004 (13%) and 2007 (17%) say other IT projects take a higher priority than full testing of the DR plan, compared to 2003 (6%).
- In contrast, more of those questioned in 2007 (12%) say full scenario DR testing is not seen as a priority by top management, compared to 2003 (2%) and 2004 (7%).
- Whereas, more of those questioned in 2004 (16%) say none of these present barriers to full scenario testing of their DR plan, compared to in 2003 (12%) and 2007 (11%).



3.11 Have you discussed and agreed acceptable levels of risk with the non-IT, business directors in the organisation?



- Just 33% of IT managers have discussed and agreed acceptable levels of risk with the non-IT, business directors within their organisation for all the threats they feel exposed to – 65% have not.
- Another 56% have had such agreements with non-IT, business directors for some of the threats they are exposed to.
- In contrast, 9% have not discussed nor agreed acceptable levels of risk for any threats.
- Another 2% are unsure.

"Agreement was reached after several meetings with company directors." Germany, IT Director, 500 employees, automotive sector.

"We discussed all the possible risks together. We have reached an agreement with the general manager." Germany, IT Manager, 800 employees, public sector.

"We talked about all the possible risks with them that our company may be exposed to, i.e. human error, which may result in data loss... power cuts, natural disasters etc. We obviously reached an agreement with the administration director." Italy, IT Director, 550 employees, public sector.

"We reached an agreement with the directors." Israel, IT Manager, 500 employees, banking sector.

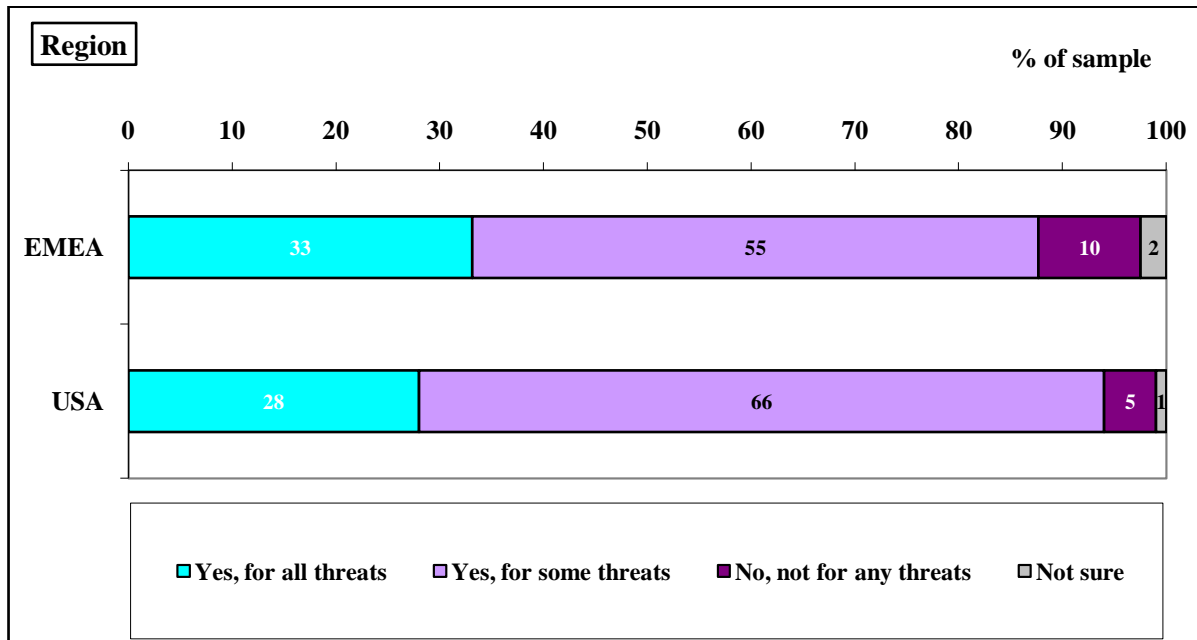
"We discussed it all with the general manager and have reached an agreement with him about all the possible threats." Israel, IT Manager, 1,000 employees, public sector.

"There is the risk manager who deals with the risks to the business and who has regular meetings with the business directors and there is a risk log and some risks are discussed monthly and some are discussed quarterly... All types of threats and levels of disaster [have been discussed], e.g. losing power on the 1st floor and moving floors to another and partly operating the IT systems and what would happen if we took out a key part of the infrastructure or just part of it out. (Researcher - Have you reached agreement?) Yes." UK, IT Manager, 1,400 employees, public sector.

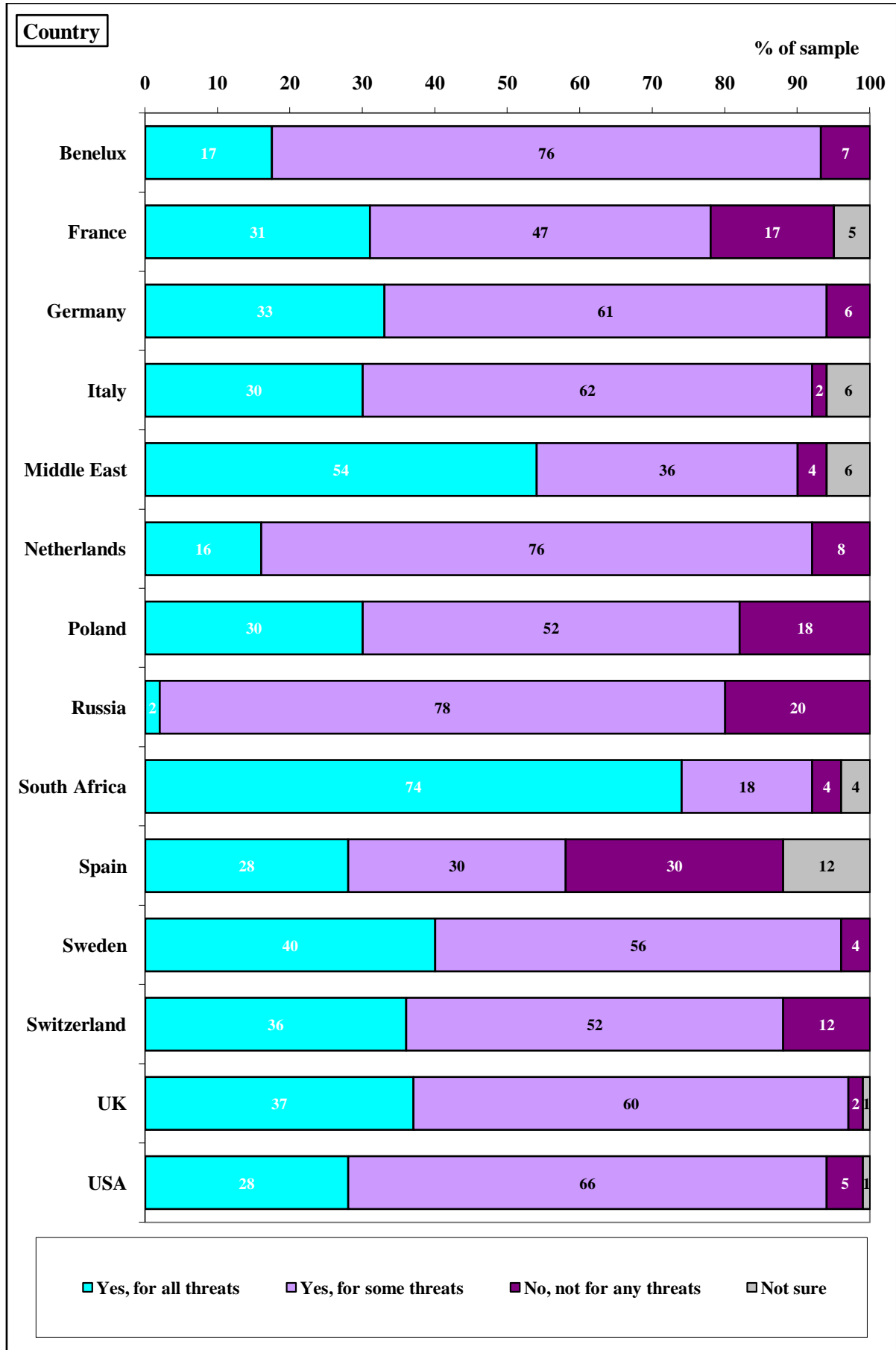
"IT and other directors have discussed the social risks and effects, potential technological damage and the possible cost consequences." Russia, IT Director, 3,450 employees, power and energy sector.

"I made the decisions myself. I have not agreed it with anyone." Israel, IT Manager, 3,000 employees, public sector.

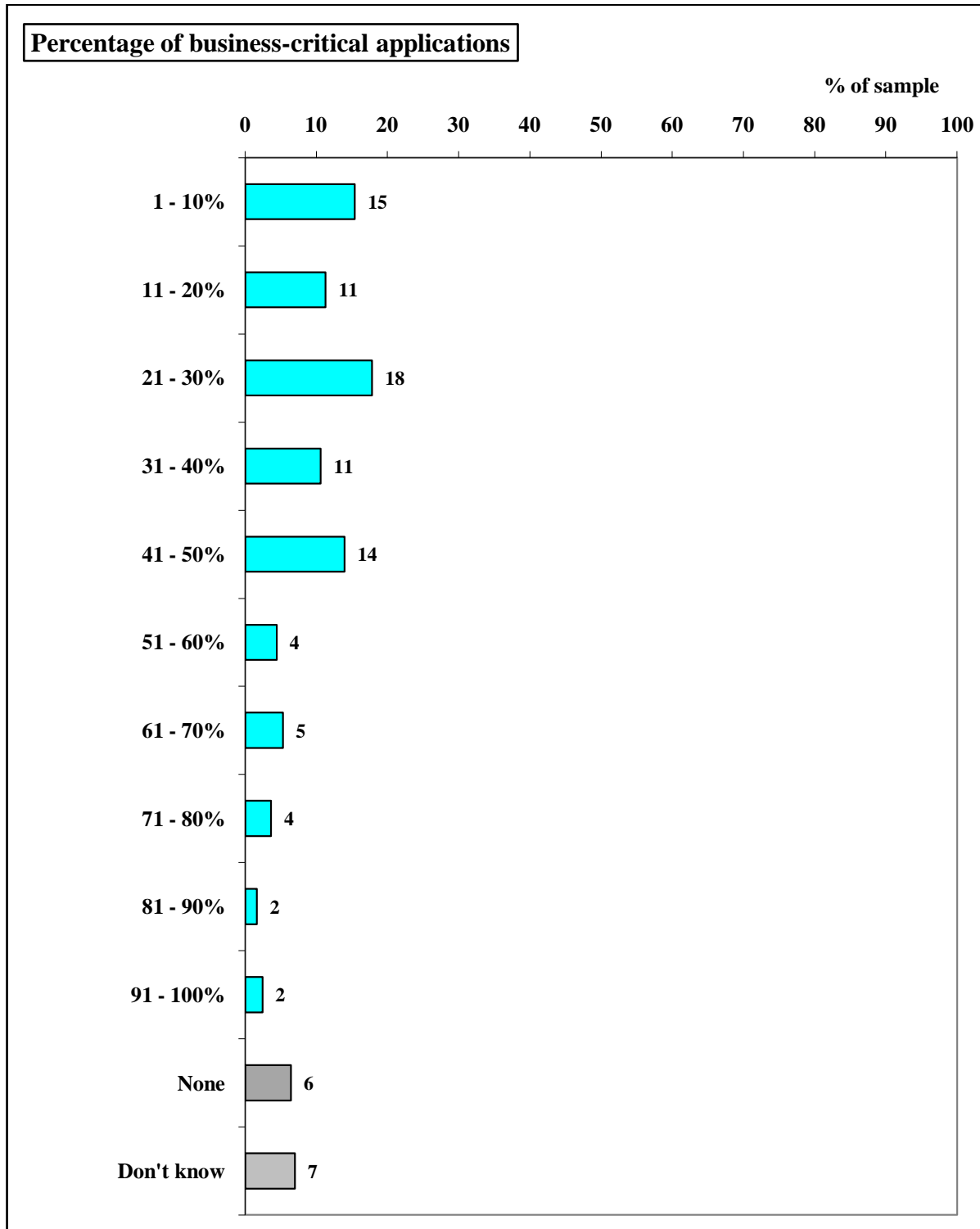
"No, we didn't have any discussions with other management." USA, IT Manager, 3,500 employees, public sector.



- More US IT managers (66%) have discussed and agreed acceptable levels of risk with the non-IT, business directors within their organisation for just some of the threats they feel exposed to, compared to EMEA organisations (55%).



3.12 What percentage of your organisation’s applications does it consider to be business-critical?



- Collectively, 94% of organisations consider at least some of their applications to be business-critical.
- On average, 36% of an organisation’s applications are deemed business-critical, and the median is 30%, but this ranges from 1-100% [not shown].

- Opinion is quite varied, but in general, more organisations (69%) cite a figure of 50% or below.
- Only 17% cite a figure above 50%.
- In contrast, 6% say none of their applications are considered business-critical.
- And 7% are unsure of the percentage of business-critical applications their organisation has.

"The servers in the finance department. That covers all of our company's business. (Researcher - Is that 100% then?) Yes. That is - 7 years' worth of data." UK, IT Manager, 670 employees, public sector.

"I'd say 95%." UK, IT Manager, 1,400 employees, public sector.

"90%." Germany, IT Manager, 2,500 employees, public sector.

"70%-75%." Jordan, IT Manager, 4,000 employees, banking sector.

"70%." Italy, IT Director, 500 employees, public sector.

"50%." USA, IT Manager, 900 employees, public sector.

"45% are critical." Germany, IT Director, 500 employees, automotive sector.

"We have about 6 systems on our business critical list. 25% of the business as a whole." UK, IT Manager, 500 employees, telecoms sector.

"10%." Russia, IT Director, 2,330 employees, power and energy sector.

"10%." USA, IT Manager, 1,500 employees, local and federal government.

"Very small." Italy, IT Manager, 3,000 employees, banking sector.

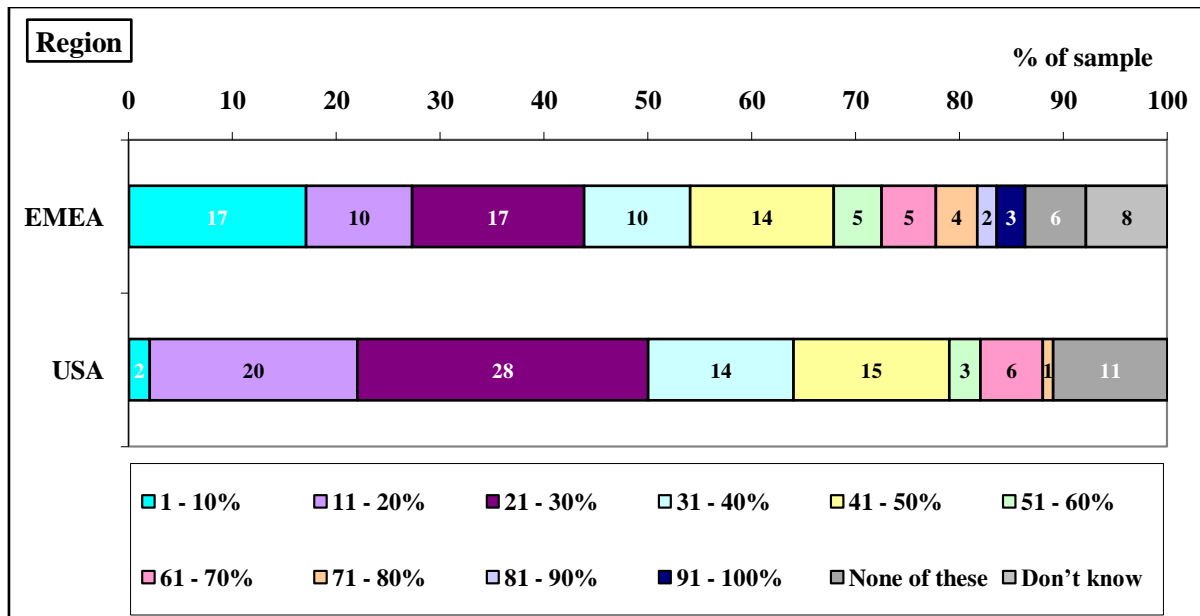


Table 15: Percentage of applications that are deemed business-critical: regions

Region	Average	Median	Range
EMEA	36%	30%	1% to 100%
USA	33%	26%	10% to 75%

- More EMEA organisations (94%) consider at least some of their applications to be business-critical, compared to US organisations (89%).
- And, more EMEA organisations (19%) consider over 50% of their applications to be business-critical, compared to US organisations (10%).
- Conversely, more US organisations (79%) say 50% or less of their organisation's applications are deemed business-critical, compared to EMEA organisations (68%).
- But, more EMEA organisations (17%) say 1-10% of their organisation's applications are deemed business-critical, compared to US organisations (2%).
- However, more US organisations (20%) say 11-20% of their organisation's applications are deemed business-critical, compared to EMEA organisations (10%).
- And, more US organisations (28%) say 21-30% of their organisation's applications are deemed business-critical, compared to EMEA organisations (17%).

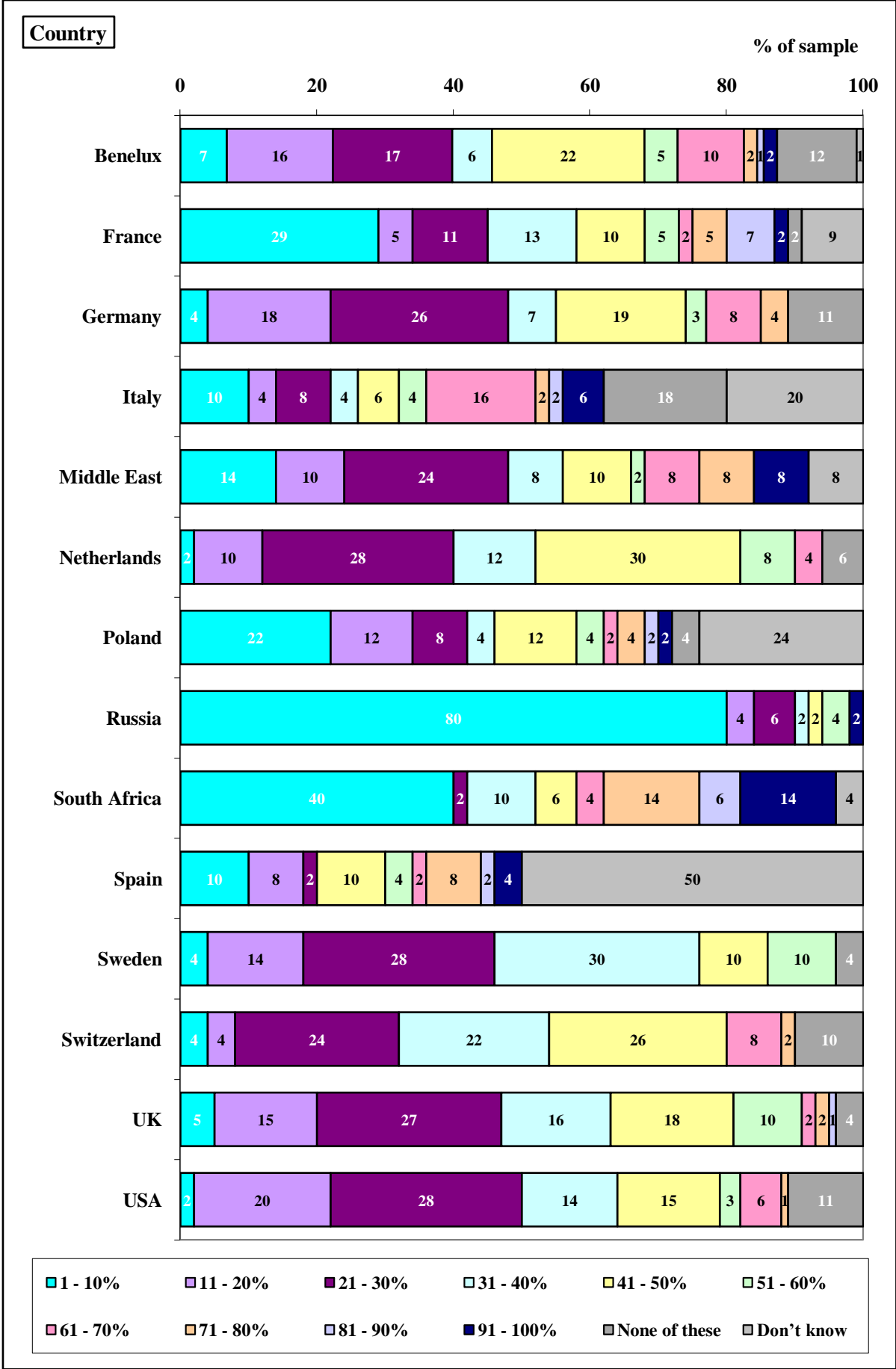
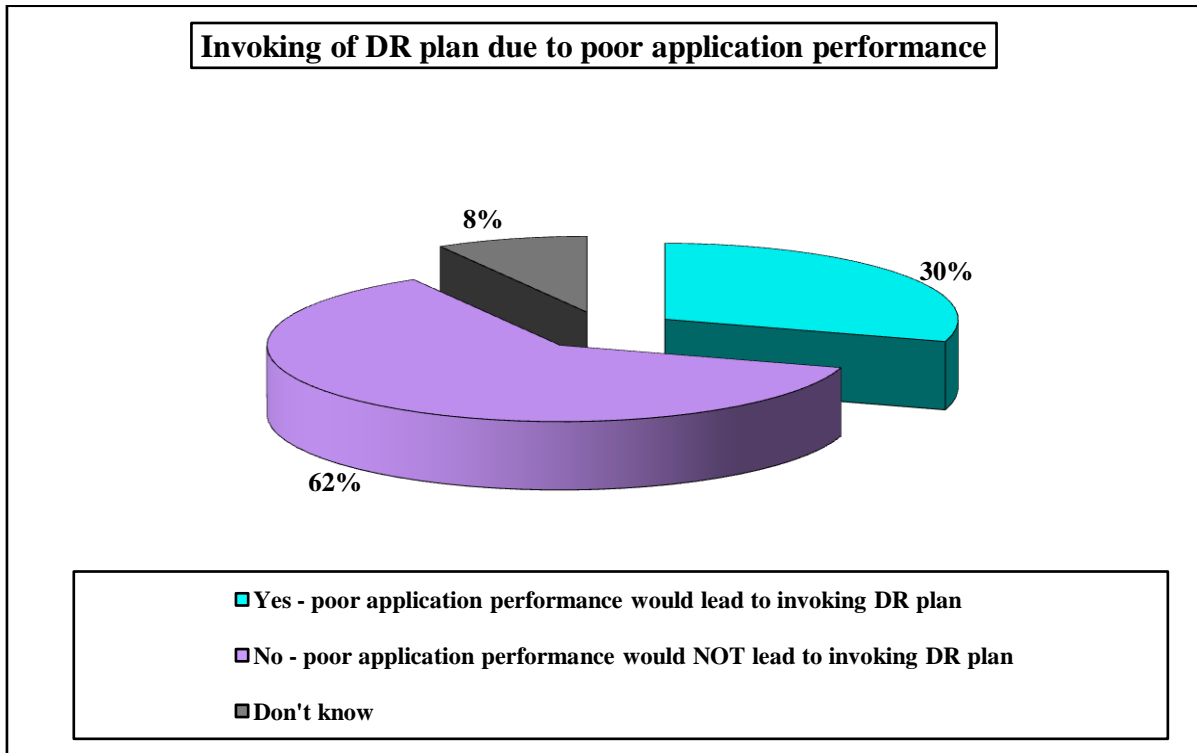


Table 16: Percentage of applications that are deemed business-critical: countries

Country	Average	Median	Range
Benelux	39%	40%	5% to 100%
France	35%	30%	1% to 100%
Germany	36%	30%	5% to 80%
Italy	51%	50%	3% to 100%
Middle East	42%	30%	1% to 100%
Netherlands	37%	40%	10% to 70%
Poland	33%	28%	2% to 100%
Russia	13%	6%	1% to 95%
South Africa	45%	40%	1% to 100%
Spain	47%	45%	2% to 100%
Sweden	32%	34%	5% to 60%
Switzerland	38%	36%	5% to 80%
UK	35%	34%	5% to 90%
USA	33%	26%	10% to 75%

3.13 Would poor application performance lead to the organisation invoking its DR plan?



- 30% of organisations say that poor application performance would lead to them invoking their DR plan.
- In contrast, 62% say this would not be the case.
- Another 8% are unsure if poor application performance would lead to invoking their plan or not.

"Yes, if all employees were to start working at the same time, the whole system would crash due to system overload so the DR plan would come into place." Germany, IT Manager, 100,000 employees, automotive sector.

"Yes, if business and its operations were affected because of poor application performance." Israel, IT Manager, 1,000 employees, public sector.

"Yes, this undermines company performance and thus undermines the safety or reputation of the organisation." Russia, IT Director, 575 employees, public sector.

"Yes, any application underperformance is a part of the DR plan." Russia, IT Director, 3,450 employees, power and energy sector.

"Yes, the DR plan, as with anything else, should justify the investment." Russia, IT Director, 560 employees, public sector.

"Possibly. It would really depend on how serious the problem is and what potential damage could be caused." USA, IT Manager, 510 employees, public sector.

"No. Well, only in extreme circumstances. Well, they'd look for routine technical resolution rather than invoke the disaster recovery plan." UK, IT Manager, 1,400 employees, public sector.

"No, because the disaster recovery plan is intended only for the case of a real disaster and not for poor application performance." Germany, IT Manager, 3,500 employees, manufacturing sector.

"No, because the disaster recovery plan would be used only in case of fire or flood, for example." Italy, IT Manager, 1,600 employees, banking sector.

"No, because poor application performance is a different sort of emergency; it is nothing to do with the DR plan." Italy, IT Manager, 3,000 employees, banking sector.

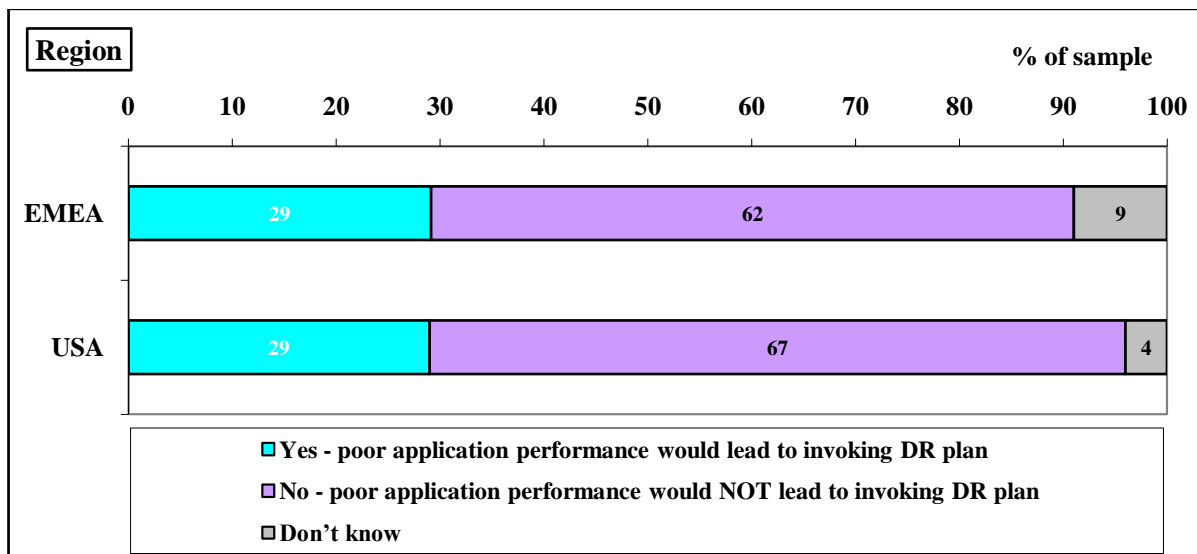
"No, there is no connection between poor application performance and the disaster recovery plan." Israel, IT Manager, 500 employees, banking sector.

"No, because disaster recovery would come in to effect only following a real disaster, like an earthquake or fire." Jordan, IT Manager, 4,000 employees, banking sector.

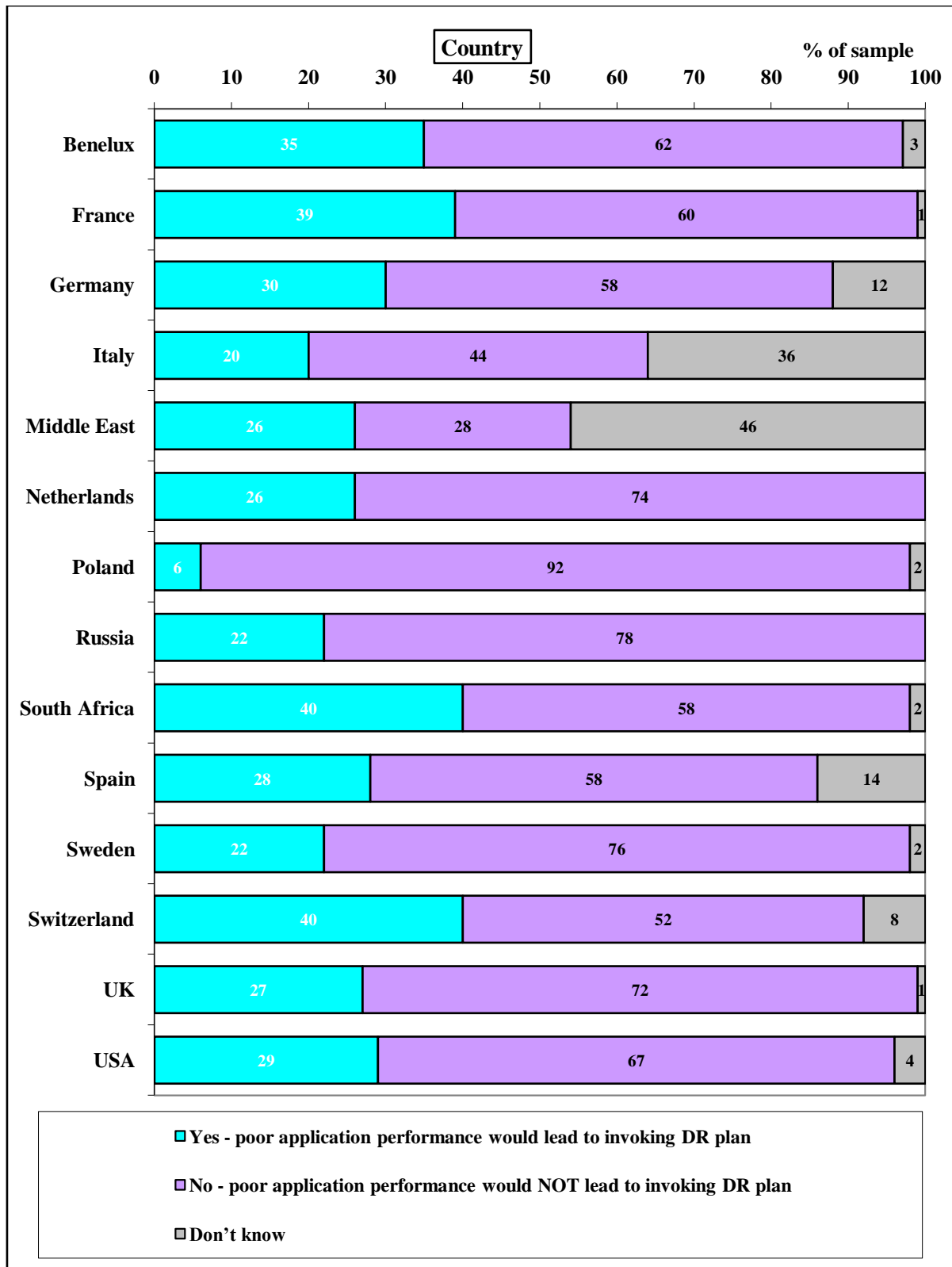
"No, because it is not a disaster. Loss of application would lead to invoking DR, but not poor application performance." UK, Head of IT, 160,000 employees, banking sector.

"Definitely not. Our DR plan is a last resort after all other avenues have been attempted." Saudi, IT Manager, 1,000 employees, public sector.

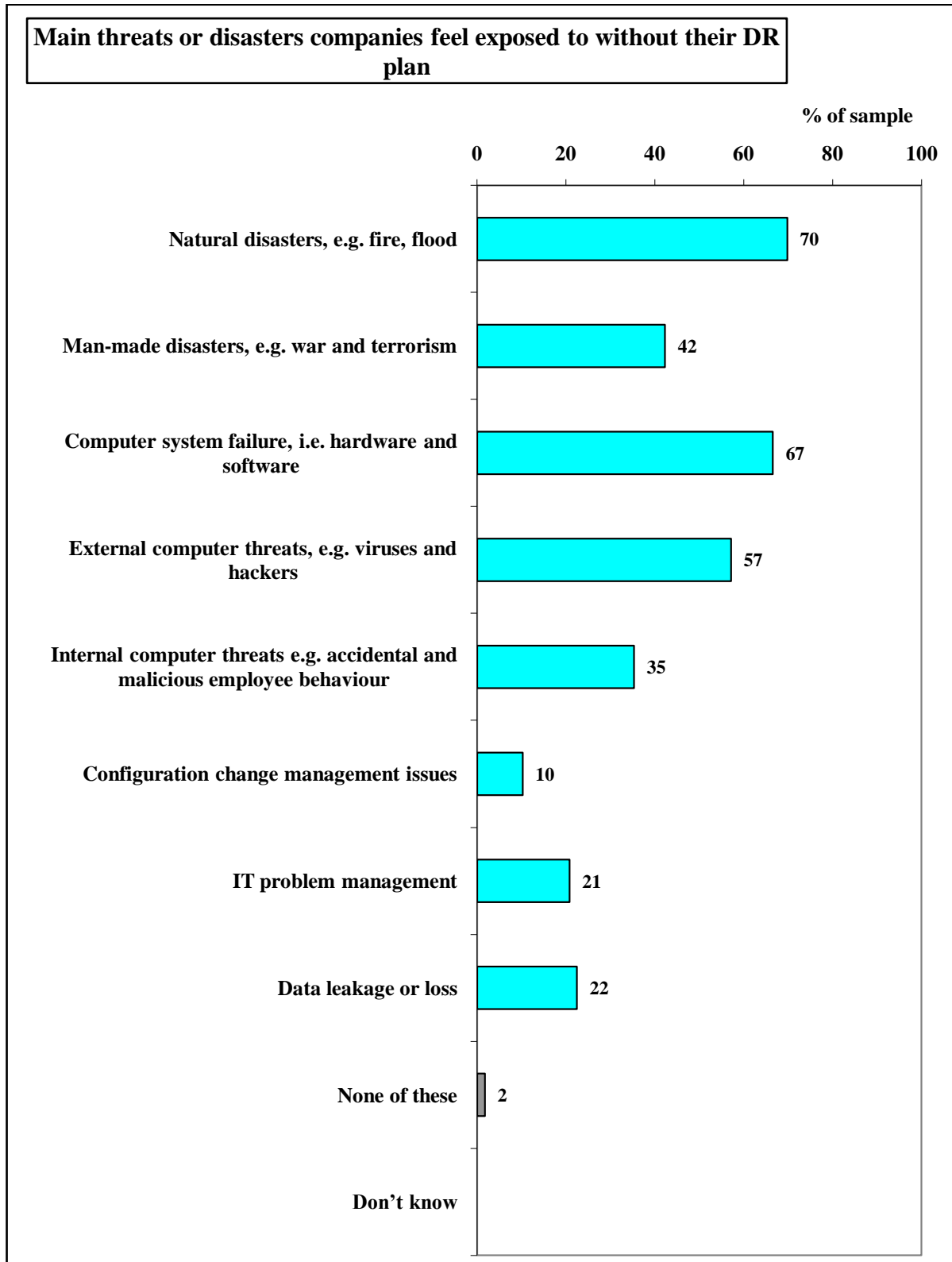
"I wouldn't have thought so because we're behind the times because we don't have online service delivery which we are currently looking into getting. It'll happen in a year or two. We're now starting to look at 24/7 electronic cover." UK, IT Manager, 2,500 employees, public sector.



- Statistically, there is no significant difference according to region and whether poor application performance would lead to the organisation invoking its DR plan.



3.14 Without your DR plan, which of the following threats or disasters would your organisation consider itself exposed to?



- Collectively, 98% of organisations would feel exposed to at least 1 of these threats or disasters if they did not have their DR plan in place.

- The Top 3 threats or disasters they would feel exposed to are:
 1. Natural disasters, e.g. fire and flood (70%)
 2. Computer failure, i.e. hardware and software (67%)
 3. External computer threats, e.g. viruses and hackers (57%)
- In addition, 42% would feel exposed to man-made disasters, such as war and terrorism, without their plans.
- But a significant number (35%) would feel exposed to internal computer threats, such as accidental and malicious employee behaviour, without their plans.
- 22% would feel vulnerable to data leakage or loss and a similar proportion (21%) would worry about IT problem management.
- Only 10% would feel exposed to configuration change management issues if they did not have their DR plans in place.
- Just 2% say they would not feel exposed to any of these threats if they did not have their DR plans.

"Hardware malfunction, fire and electricity blackout." Germany, IT Manager, 800 employees, public sector.

"Without a DR plan, the company may be exposed to ANY possible threat; terrorist attacks, electrical, or human error." Italy, IT Manager, 1,600 employees, banking sector.

"Without the disaster recovery plan, we couldn't start normal operation immediately, which would lead to poor customer service and damage to the brand image." Italy, IT Manager, 3,000 employees, banking sector.

"Fire, system theft, loss of financial data." Saudi, IT Manager, 1,000 employees, public sector.

"Terror acts, political instability and power loss." Israel, IT Manager, 3,000 employees, public sector.

"Fire, natural disasters and winter weather conditions mainly." Russia, IT Director, 2,330 employees, power and energy sector.

"The threat of power cuts or the threat of terror acts, like a bomb explosion, and then there is fire or human error." Russia, IT Director, 510 employees, public sector.

"Fire, flood, theft of equipment: general problems any business would have - staff destroying and corrupting data. The risk of a plane landing on us is nil because we are not in a flight path." UK, IT Manager, 670 employees, public sector.

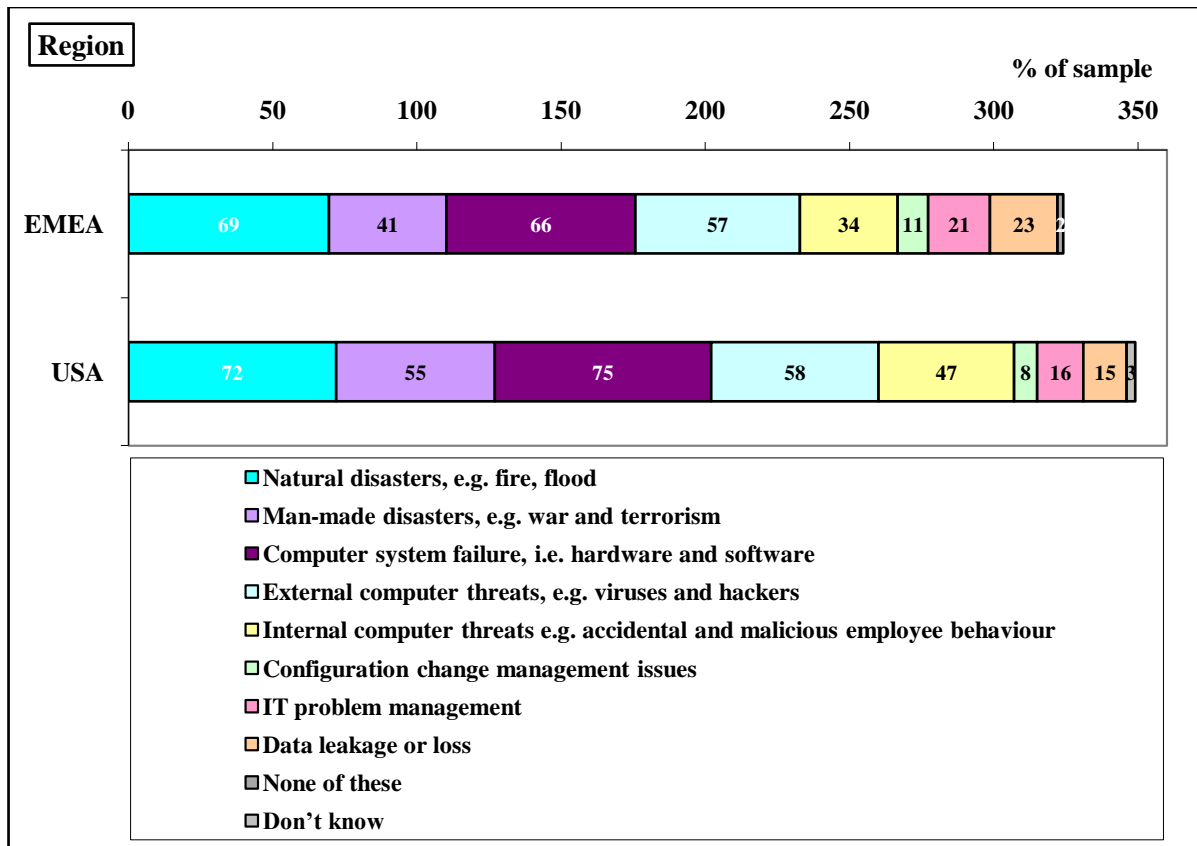
"Floods, fires and all those things." UK, IT Manager, 10,000 employees, banking sector.

"Hacking because it's a telecoms networks company so that is always the main threat. (Researcher - Anything else?) Hacking is the main worry." UK, IT Manager, 500 employees, telecoms sector.

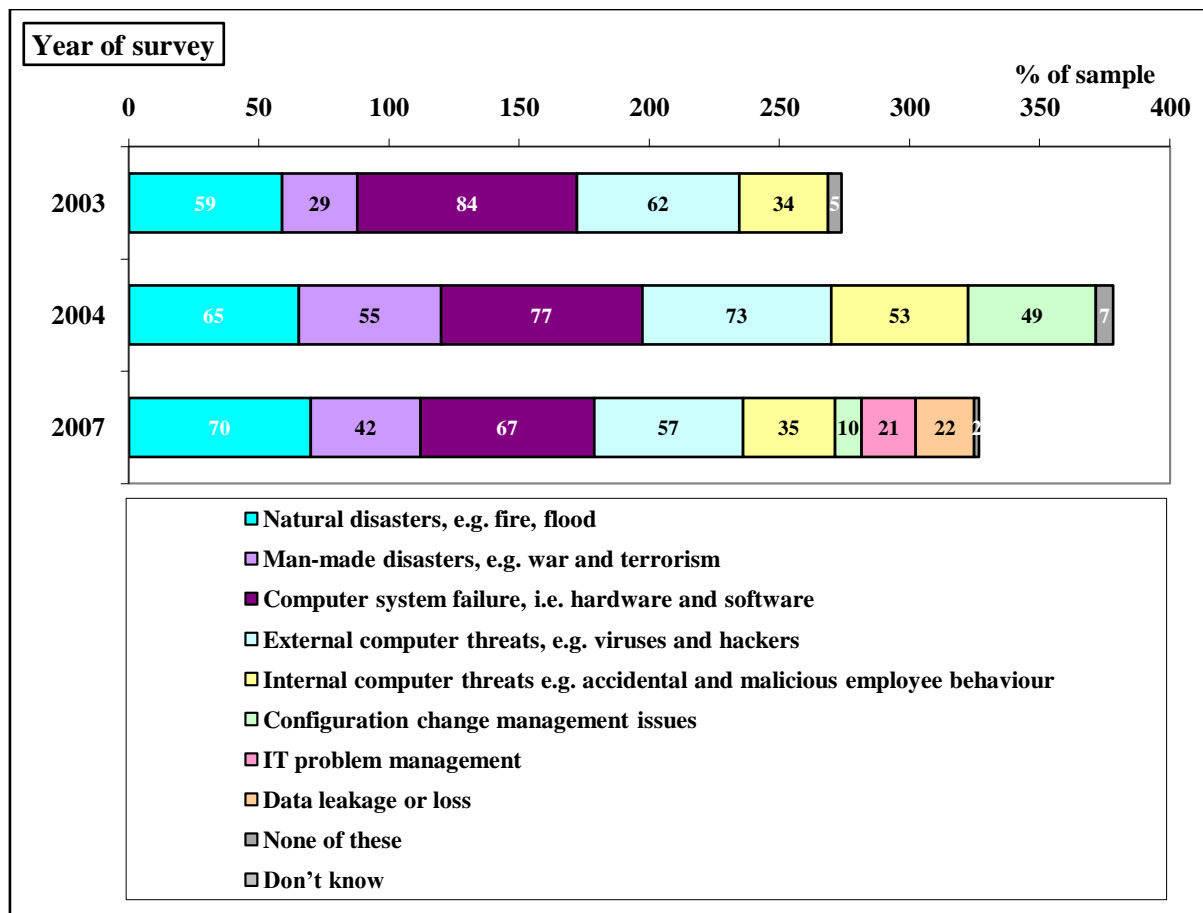
"We would be worried about the possibility of power cuts, natural disasters and potential terrorist threats." USA, IT Manager, 1,500 employees, local and federal government.

"Malfunction of the CPU, burglary and vandalism are the top 3." USA, IT Manager, 510 employees, public sector.

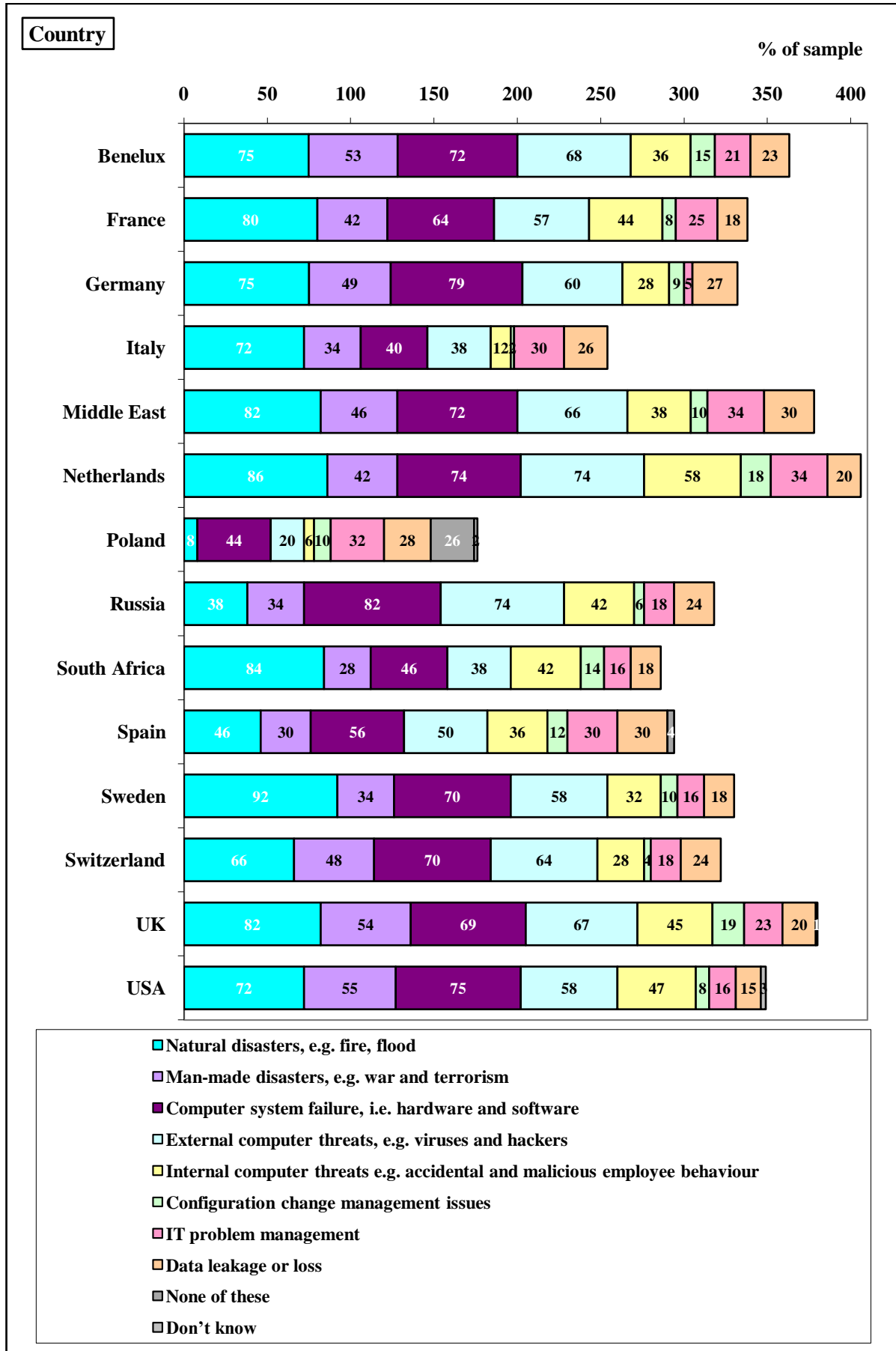
"Severe weather conditions, fire and power cuts are the main ones." USA, IT Manager, 900 employees, public sector.



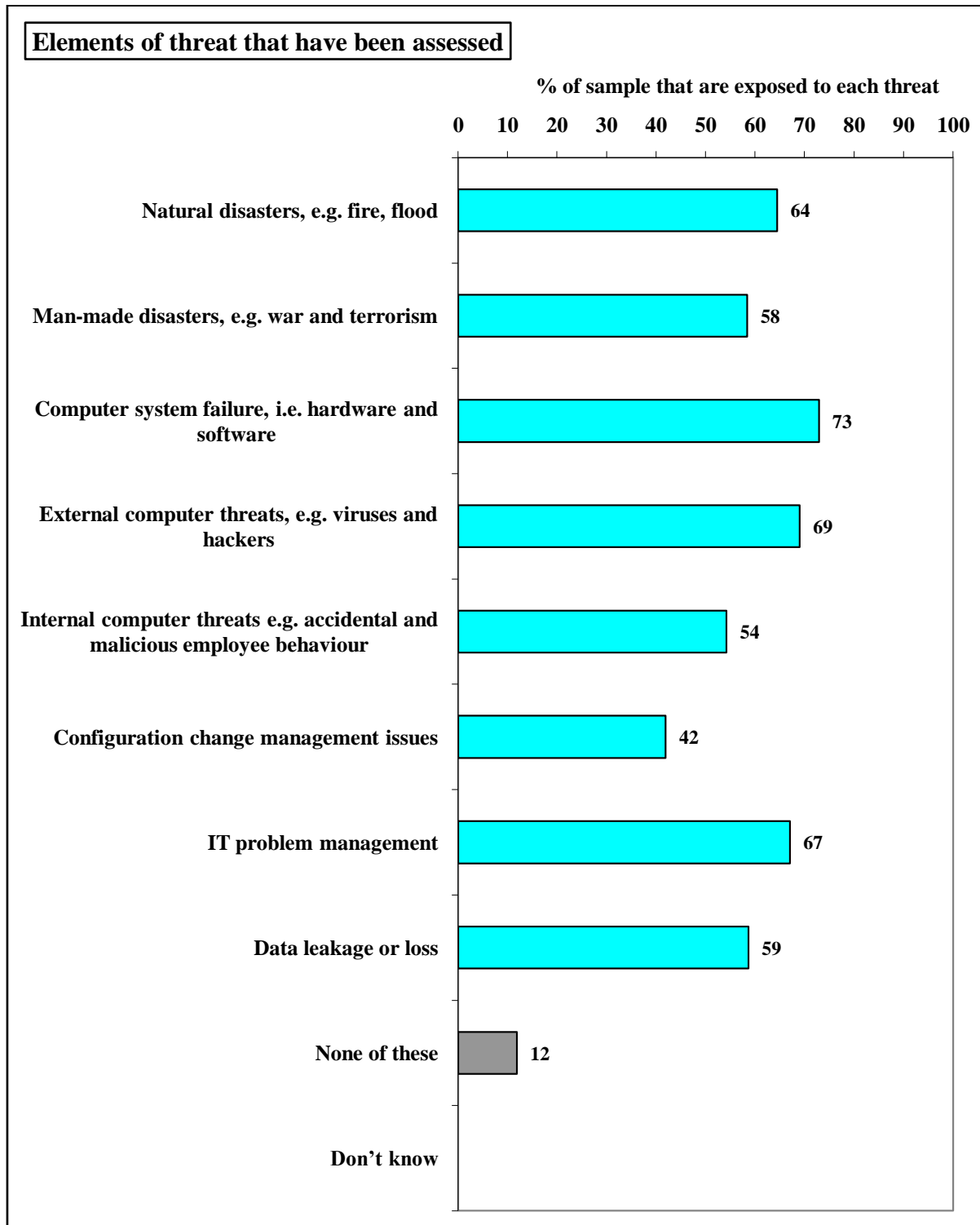
- More US organisations (76%) would feel exposed to 3 or more of these threats or disasters if they did not have their DR plan in place, compared to EMEA organisations (64%) [not shown].
- In detail, more US organisations (55%) would feel exposed to man-made disasters, such as war and terrorism, without their plans, compared to EMEA organisations (41%).
- Also, more US organisations (47%) would feel exposed to internal computer threats, such as accidental and malicious employee behaviour, without their plans, compared to EMEA organisations (34%).



- Overall, organisations questioned in 2004 say their organisation would consider itself exposed to more of these threats or disasters without their DR plans, compared to the other years (i.e. length of bars in the above chart)
- In fact, more organisations questioned in 2007 (98%) would feel exposed to at least 1 of these threats or disasters if they did not have their DR plan in place, compared to organisations questioned in 2003 (95%) and 2004 (93%).
- In detail, more organisations questioned in 2007 (70%) would feel exposed to natural disasters, such as fire and flood, compared to organisations questioned in 2003 (59%) and 2004 (65%).
- But, more organisations questioned in 2004 (55%) would feel exposed to man-made disasters, compared to 2003 (29%) and 2007 (42%).
- Yet, more organisations questioned in 2003 (84%) would feel exposed to computer failure, compared to 2004 (77%) and 2007 (67%).
- Whereas, more organisations questioned in 2004 (73%) would feel exposed to external computer threats, compared to 2003 (62%) and 2007 (57%).
- And, more organisations questioned in 2004 (53%) would feel exposed to internal computer threats, compared to 2003 (34%) and 2007 (35%).
- However, more organisations questioned in 2003 (5%) and 2004 (7%) say they would not feel exposed to any of these threats if they did not have their DR plans, compared to organisations questioned in 2007 (2%).



3.15 [Just to those exposed to threats without their DR plans] For which of these threats has your organisation carried out a probability and impact assessment?



- Collectively, 88% of organisations have carried out a probability and impact assessment for at least 1 of these threats.

- Indeed, 65% have carried out such assessments for 3 or more, but only 24% have done them for 5 or more [not shown].
- However, only 40% have carried out a probability and impact assessment for all the threats they feel exposed to (as cited in Section 3.14) [not shown].
- And 12% have not carried out an impact and assessment study for any of the threats they feel exposed to [not shown].
- The 3 most commonly assessed threats are:
 4. Computer system failure (73%)
 5. External computer threats (69%)
 6. IT problem management (67%)
- In addition, 64% of organisations that feel exposed to natural disasters have carried out a probability and impact assessment for this threat.
- Just 59% of organisations that feel exposed to data leakage or loss have carried out a suitable assessment for this threat.
- A similar proportion (58%) that feel exposed to man-made disasters, like war and terrorism, have carried out such assessments for this threat.
- And 54% of those that feel exposed to internal computer threats have carried out these necessary assessments for this threat.
- The least assessed area is for configuration change management issues, where only 42% of people that feel exposed to this threat have carried out a probability and impact assessment.

"We carried out probability assessment tests for all the threats we feel exposed to. In case the central database is not internally accessible, we have to move into another branch." Italy, IT Manager, 800 employees, banking sector.

"Yes, for all of them." Israel, IT Manager, 3,000 employees, public sector.

"Yes, of course we did." Israel, IT Manager, 1,000 employees, public sector.

"Yes, we did a very detailed test on the possible technological effects and impacts." Russia, IT Director, 3,450 employees, power and energy sector.

"Again, in the quarterly or monthly meeting we have, the risks are assessed from very low to very high and the business impact from extremely critical to very low. We really have 5 probabilities and the impacts range from negligible to catastrophic, so that's 5 levels of risk too. We have assessed all of them." UK, IT Manager, 1,400 employees, public sector.

"Only on some, but not fully for all. We have done it on the assessment of human error, and on computer theft. As we discussed earlier, we have assessed the impact with regards to costs, and timings." Russia, IT Director, 560 employees, public sector.

"We set up a drill of what would happen if there is no electricity for one day and assessed exactly how bad and in which areas the company would be affected most." Germany, IT Director, 500 employees, automotive sector.

"Yes, we did carry out a probability test; in the case of water, fire and electricity disasters." Germany, IT Manager, 3,500 employees, manufacturing sector.

"No. Not for any, actually." Italy, IT Director, 500 employees, public sector.

"No." Germany, IT Manager, 2,500 employees, public sector.

"No." UK, Head of IT, 160,000 employees, banking sector.

"Err, no." Jordan, IT Manager, 4,000 employees, banking sector.

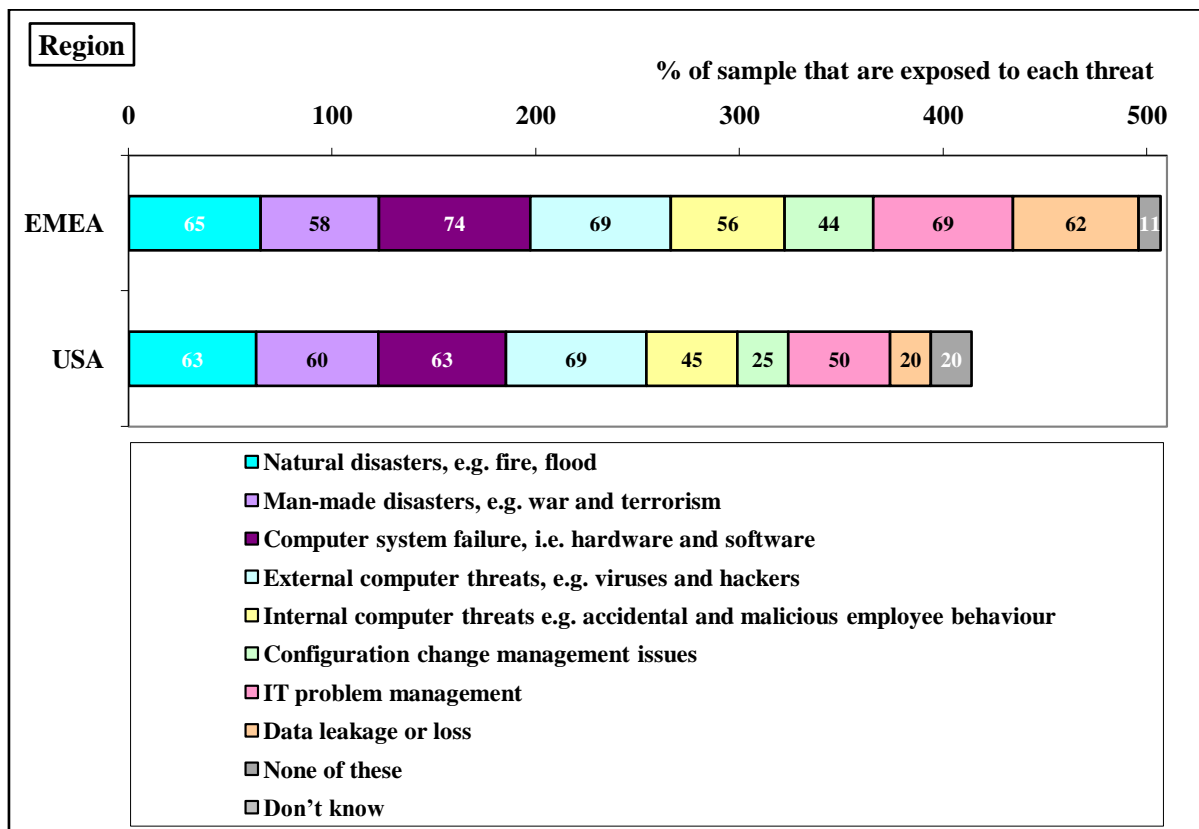
"No we didn't carry out such an assessment on the threats that we are exposed to." Saudi, IT Manager, 1,000 employees, public sector.

"No. Can't say we did." Russia, IT Director, 2,330 employees, power and energy sector.

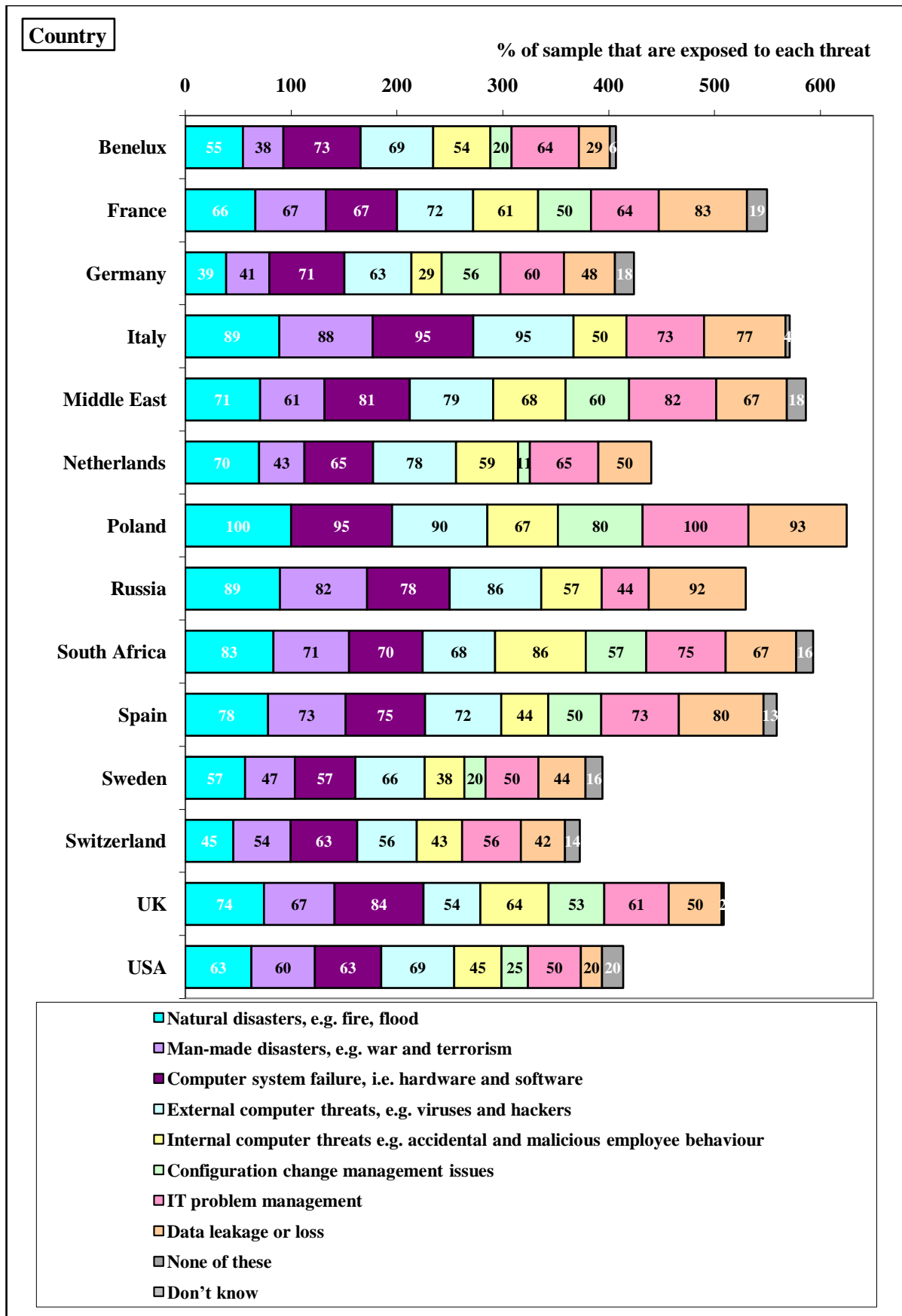
"No, we have not carried out any probabilities or impact assessments." USA, IT Manager, 1,500 employees, local and federal government.

"Not yet." Israel, IT Manager, 500 employees, banking sector.

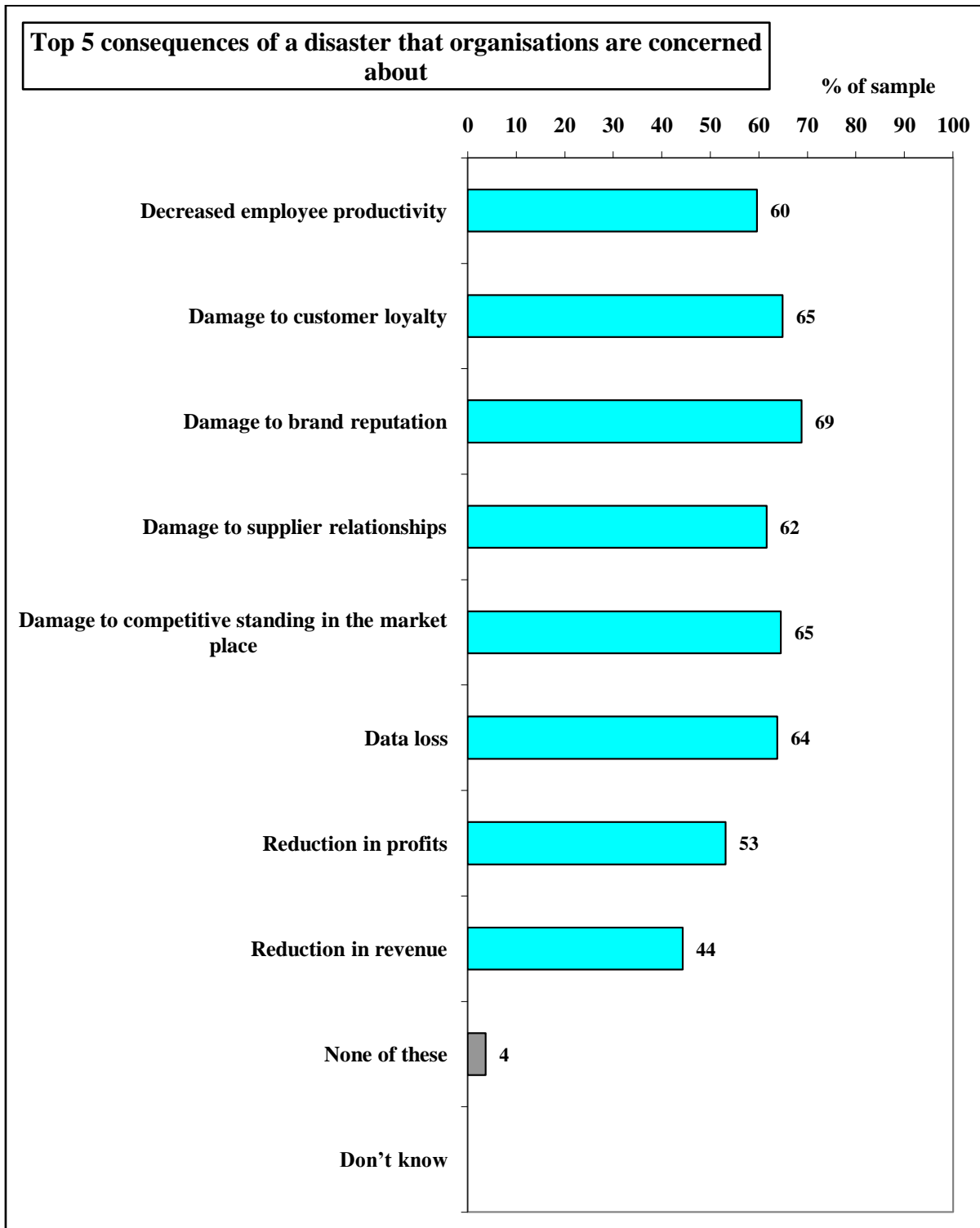
"We have not tested it yet, but we are happy with the level of security we have implemented." USA, IT Manager, 1,000 employees, investment banking sector.



- Overall, EMEA organisations have carried out a probability and impact assessment for more of the threats they feel exposed to, compared to US organisations (i.e. length of bars in above chart).
- Indeed, more EMEA organisations (89%) have carried out a probability and impact assessment for at least 1 of these threats, compared to US organisations (80%).
- In fact, more US organisations (55%) have not carried out a probability and impact assessment for all the threats they feel exposed to, compared to EMEA organisations (38%) [not shown].
- In detail, more EMEA organisations that feel exposed to computer system failure (74%) have carried out an assessment for this threat, compared to US organisations (63%).



3.16 Which 5 of the following potential impacts or consequences that could result from a disaster is your organisation most concerned about?



- Collectively, 96% of IT managers say their organisation is concerned about at least 1 of these potential impacts or consequences that could result from a disaster.

- Indeed, all potential impacts and consequences are popular concerns (all 44-69%) with none standing out significantly above the rest.
- However, at the top of the list is damage to brand reputation (69%).
- This is followed by 65% who fear damage to customer loyalty and the same amount fear damage to their competitive standing in the market place.
- Almost as many (64%) are concerned about data loss as a potential impact or consequence of a disaster.
- But 62% worry about damage to supplier relationships and 60% worry about decreased employee productivity.
- Slightly fewer (53%) say they are concerned about a reduction in profits and fewer still (44%) worry about a reduction in revenue.
- In contrast, 4% say they are not concerned about any of these potential impacts or consequences as a result of a disaster.

"If this [loss of data] were to happen, it would affect our daily operation and our credibility."
USA, IT Manager, 510 employees, public sector.

"The worst consequence would be to lose the data, which leads to damage to the brand."
Jordan, IT Manager, 4,000 employees, banking sector.

"Obviously the loss of information, then there would be a high cost in getting the system stable and recovering the data; and then there would be the damage to the company's reputation."
Russia, IT Director, 510 employees, public sector.

"We would be unable to do business. There would be reputation issues." UK, IT Manager, 10,000 employees, banking sector.

"The worst impact would be losing the data; namely customer, financial and council data."
Germany, IT Manager, 3,500 employees, manufacturing sector.

"Potentially losing the data and afterwards the backlash could even close the company." Italy, IT Manager, 1,600 employees, banking sector.

"The main consequences are losing the data and temporarily bad customer service." Italy, IT Manager, 800 employees, banking sector.

"It would affect internal operation and the financials." Israel, IT Manager, 3,000 employees, public sector.

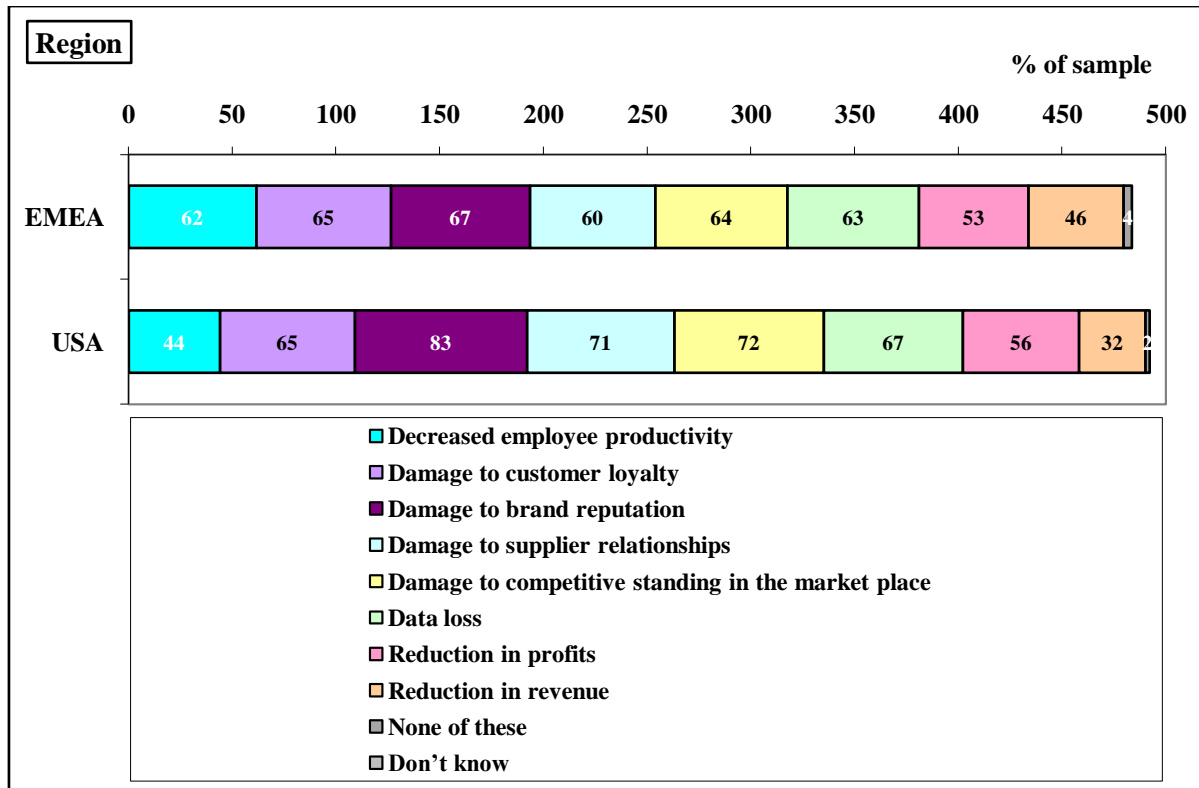
"Revenue losses and the organisation's reputation." Jordan, IT Manager, 2,000 employees, public sector.

"Due to the nature of the activity of the organisation, it is not really exposed to virus attacks or network issues. The main threats are human error, system failure and possibly fire. Thus, the likely impacts could be: loss of data, work disruption and increasing costs." Russia, IT Director, 575 employees, public sector.

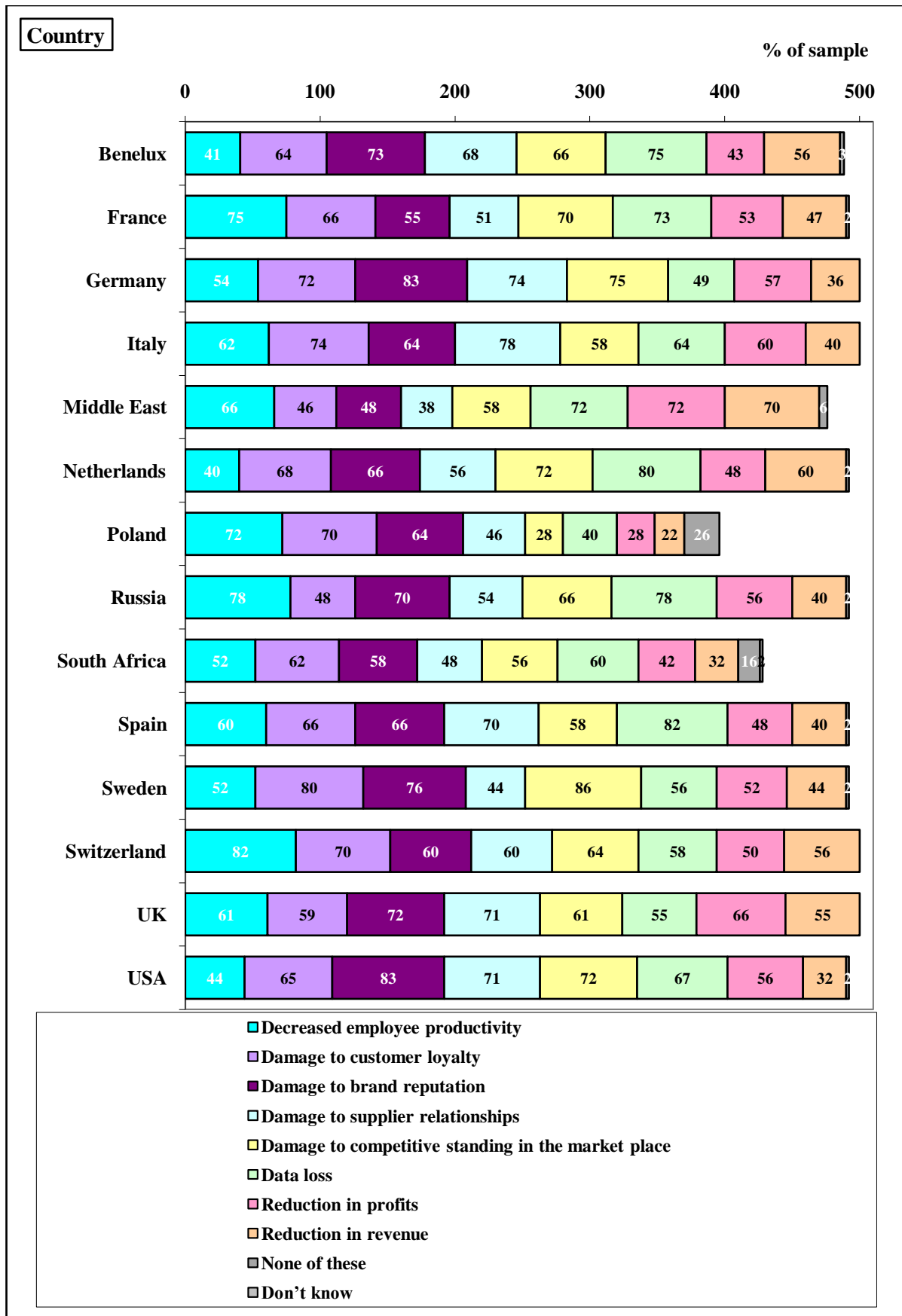
"1. Reputational risk. 2. Inability to trade. 3. Financial loss." UK, Head of IT, 160,000 employees, banking sector.

"We could face serious consequences if we lost customers' information and personal banking information. Our biggest threats are loss of custom, legal action and loss of financial input."
USA, IT Manager, 1,000 employees, investment banking sector.

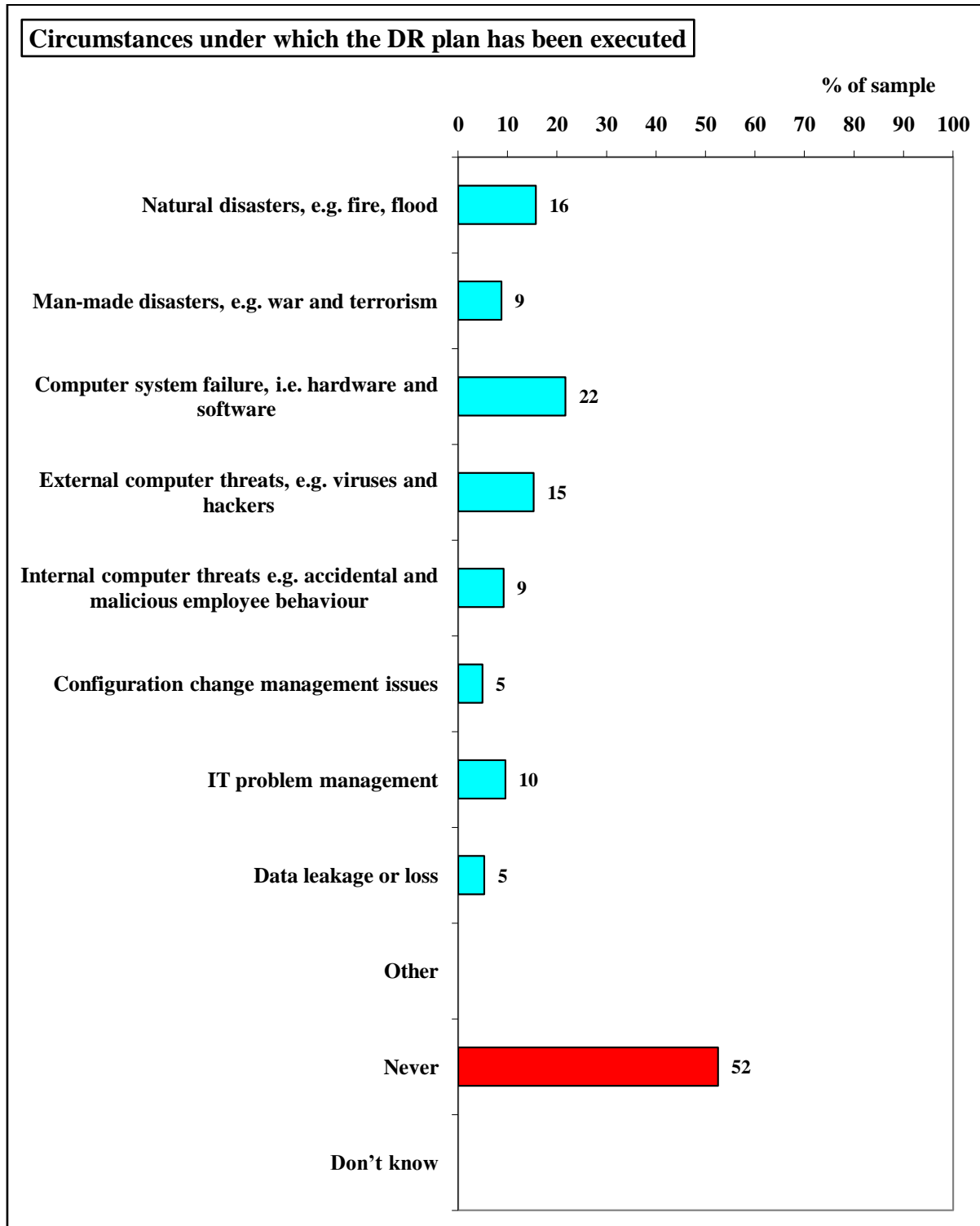
"We could lose customers and their personal information, which in the long run would make us liable for nearly 190 million dollars in compensation which would ruin us financially." USA, IT Manager, 1,800 employees, investment banking sector.



- More EMEA IT managers (62%) say their organisation is concerned about decreased employee productivity that could result from a disaster, compared to the US (44%).
- But, more US IT managers (83%) say their organisation is concerned about the damage to brand reputation, compared to EMEA (67%).
- And, more US IT managers (71%) say their organisation is concerned about the damage to supplier relationships, compared to EMEA (60%).
- However, more EMEA organisations (46%) worry about a reduction in revenue, compared to US organisations (32%).



3.17 Under what circumstances have you ever had to actually execute for real your disaster recovery plan, either in full or in part?



- Collectively, 48% of organisations have had to execute for real their DR plan, either in full or in part.
- Indeed, 26% have had to execute their plan for 2 or more of these reasons; and 12% have had to do it for 3 or more [not shown].

- The most common circumstance for DR plan execution has been computer system failure, such as hardware and software failure (22%).
- This is followed by 16% of organisations that have executed for real their DR plan due to natural disasters, such as fire and floods.
- Almost as many (15%) have executed their plans due to external computer threats, such as viruses and hackers.
- The next most common reason is due to IT problem management, which has caused 10% of organisations to execute for real their DR plan.
- But almost as many (9%) have implemented the plans due to man-made disasters, such as war and terrorism, and the same amount (9%) have executed it due to internal computer threats, such as accidental and malicious employee behaviour.
- At the bottom of the list, 5% have implemented their plans due to configuration change management issues, and the same amount (5%) have executed due to data leakage or loss.
- In contrast, 52% have never had to execute their DR plan.

"Partially during a fire; the main server crashed and the disaster recovery plan worked well, but it was slow." Israel, IT Manager, 3,000 employees, public sector.

"Yes, we had a fire on the site." Russia, IT Director, 3,450 employees, power and energy sector.

"Yes, we had power failure in the data centre." UK, Head of IT, 160,000 employees, banking sector.

"When we experienced computer system failure." Germany, IT Manager, 100,000 employees, automotive sector.

"It happened; one of the main servers got smashed." Jordan, IT Manager, 2,000 employees, public sector.

"Never." Germany, IT Director, 500 employees, automotive sector.

"No, we haven't had to execute for real the disaster recovery plan yet." Germany, IT Manager, 3,500 employees, manufacturing sector.

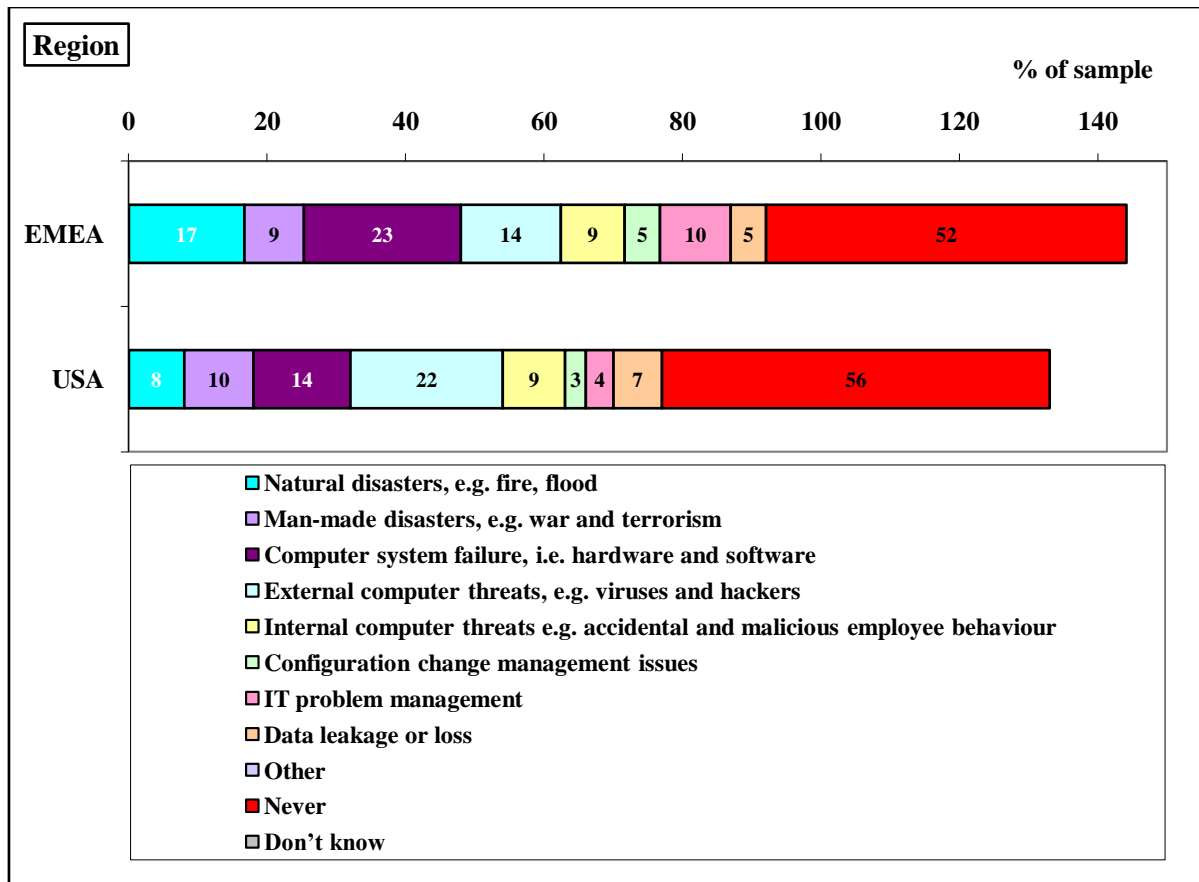
"Not yet." Italy, IT Director, 540 employees, public sector.

"Never." Israel, IT Manager, 500 employees, banking sector.

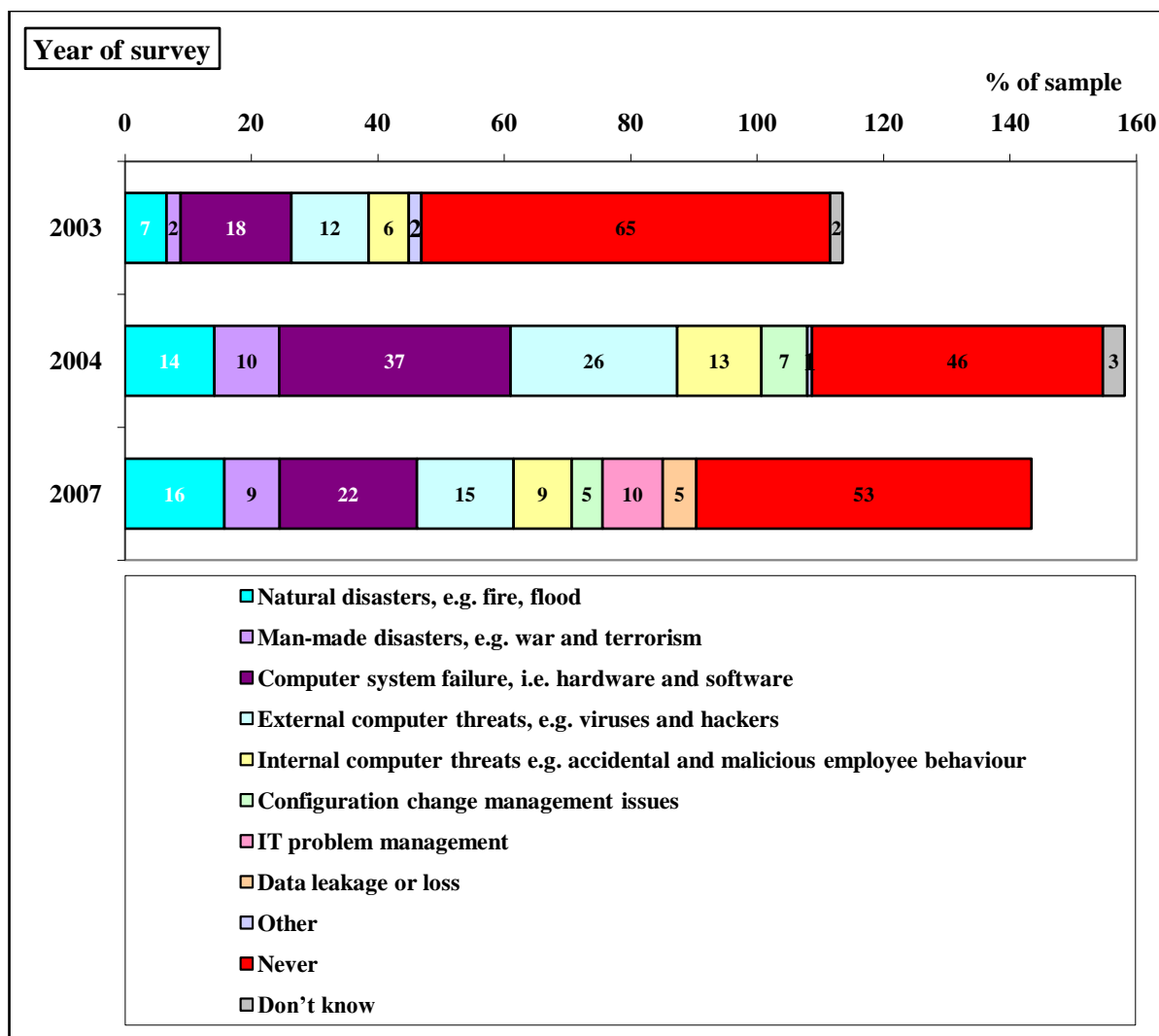
"No, fortunately we have never had to do it." Saudi, IT Manager, 1,000 employees, public sector.

"No, we have never had any such circumstances." Russia, IT Director, 2,330 employees, power and energy sector.

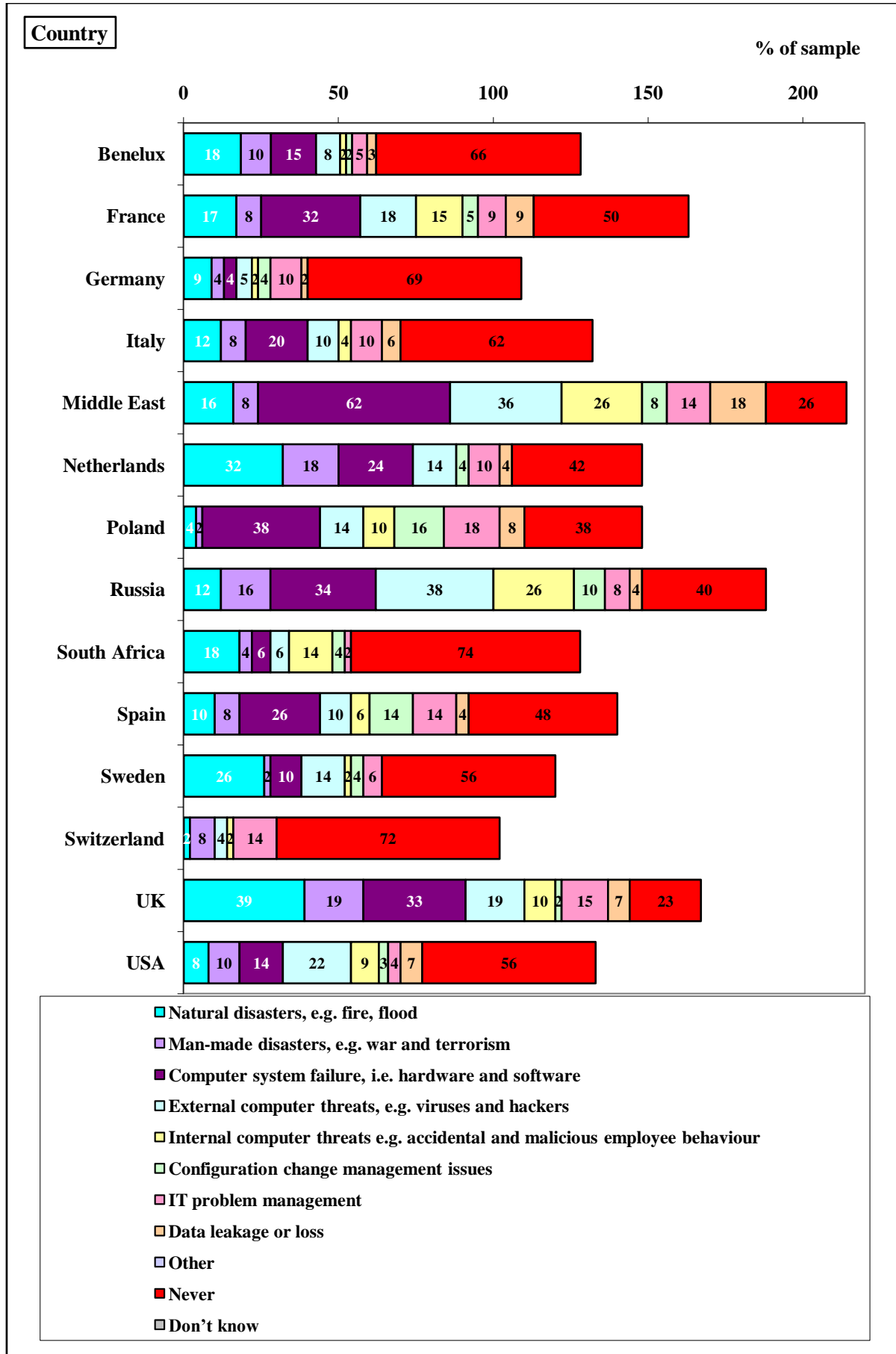
"No, we haven't executed it yet." USA, IT Manager, 510 employees, public sector.



- While similar proportions of organisations in both regions have had to execute for real their DR plans, EMEA organisations have had to do this for more of these reasons, compared to the US (i.e. length of bars in the above chart).
- In detail, more EMEA organisations (17%) have executed for real their DR plan due to natural disasters, such as fire and floods, compared to US organisations (8%).
- And, more EMEA organisations (23%) have executed their DR plan due to computer system failure, compared to the US (14%).
- But, more US organisations (22%) have executed their DR plan due to external computer threats, compared to EMEA (14%).
- Whereas, more EMEA organisations (10%) have executed their DR plan due to IT problem management, compared to the US (4%).



- More organisations questioned in 2004 (51%) and 2007 (48%) have had to execute for real their DR plan, either in full or in part, compared to organisations questioned in 2003 (33%).
- In detail, more organisations questioned in 2004 (14%) and 2007 (16%) have had to execute their DR plan due to natural disasters, such as fire and floods, compared to those questioned in 2003 (7%).
- Also, more organisations questioned in 2004 (10%) and 2007 (9%) have implemented their plans due to man-made disasters, compared to 2003 (2%).
- In addition, more organisations questioned in 2004 (37%) and 2007 (22%) have implemented their plans due to computer system failure, compared to 2003 (18%).
- But, more organisations questioned in 2004 (26%) have executed their plans due to external computer threats, compared to 2003 (12%) and 2007 (15%).
- Yet, more organisations questioned in 2004 (13%) and 2007 (9%) have implemented the plans due to internal computer threats, compared to 2003 (6%).
- In contrast, more organisations questioned in 2003 (65%) have never had to execute their DR plan for real, compared to organisations questioned in 2004 (46%) and 2007 (52%).



3.18 If you could imagine for a moment that a significant fire disaster were to occur at your organisation that obliterated the main data centre, how soon would the organisation be able to do each of the following: a) achieve skeleton operations, b) get mostly back up and running and c) have 100% normal operations?

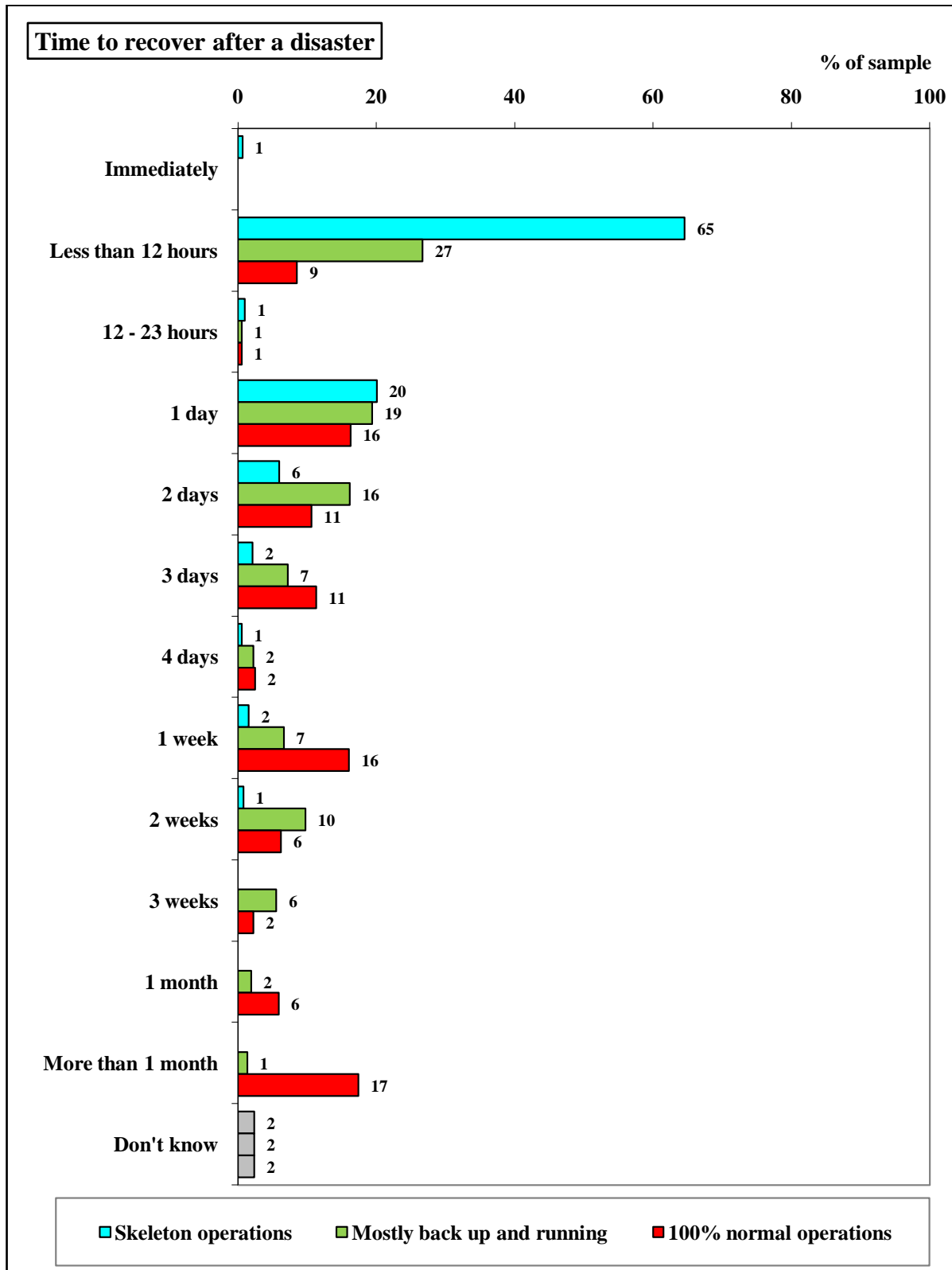


Table 17: Time needed to recover from a major fire disaster: whole sample

Operational level	Average	Median	Range
Achieve skeleton operations	0.8 days	0.2 days	Immediately to 1 month
Get mostly back up and running	5.3 days	2 days	2 minutes to 3 months
Have 100% normal operations	19 days	4 days	10 minutes to 18 months

- Only 1% of organisations could carry on with business as usual if a significant fire disaster were to occur at their organisation and completely obliterate the main data centre.

Skeleton operations:

- Collectively, 32% of organisations would need 1 day / 24 hours or longer to establish skeleton operations following such a fire disaster.
- In fact, the average time it takes for organisations to establish skeleton operations following a major fire disaster is 0.8 days, and this ranges from immediately to 1 month.
- But 66% of organisations say they could achieve skeleton operations within less than 12 hours.

Mostly up and running:

- Only 27% of organisations say they would be able to get mostly back up and running within less than 12 hours of a major fire disaster.
- The average time it takes to achieve this recovery status is 5.3 days, and the range is 2 minutes to 3 months.

100% normal operations:

- Only 9% of organisations say they would be able to get back to 100% normal operations within less than 12 hours of a major fire disaster.
- The average time it takes to achieve this recovery status is 19 days, and the range is 10 minutes to 18 months.
- But 41% would take a week or more and 17% would take more than 1 month.

"The organisation can reinstate skeleton operations immediately because we have a well-protected room with a big disaster recovery system. (Researcher - And what about achieving 100% normal operations again?) We would need about 2 hours to reinstate 100% normal operations." Italy, IT Director, 500 employees, public sector.

"We would need 1 hour to resume basic operations, leading to fully operational in up to 1 day, but more or less 10 days for 100% operations." Jordan, IT Manager, 4,000 employees, banking sector.

"We need 1-2 hours to restart again with basic operations. (Researcher - And what about achieving 100% normal operations again?) And 5 hours to resume complete operations." Italy, IT Manager, 3,000 employees, banking sector.

"For basic operations we need 3 hours. For 100%, at least one week because we need to buy new pieces of kit and organise everything." Israel, IT Manager, 500 employees, banking sector.

"We would be able to start skeleton operations with 3-4 hours of it occurring and we would be fully operational within 2 days." USA, IT Manager, 1,000 employees, investment banking sector.

"Between 2 and 7 hours – as in one working day. It depends on the level of damage done to the backup servers; it might take longer than that. (Researcher - What about getting things mostly back up and running?) From one working day to several days, depending on the level of damage." Russia, IT Director, 510 employees, public sector.

"We do need 24 hours to start everything up again completely." Germany, IT Manager, 3,500 employees, manufacturing sector.

"The plan suggests that within 24 hours we can get new PCs because our suppliers can supply in the next working day. Then I could go to the backup site and pick up the server. (Researcher - What about getting things mostly back up and running?) Within 48 hours, all the PCs will be connected and the data restored. (Researcher - And what about achieving 100% normal operations again?) With paper being irreplaceable, within a week, because it would take 10 working days to 2 weeks for the broadband and new phones to be restored. (Researcher - We are just referring to the IT stuff.) Well the broadband line at least is classified under IT." UK, IT Manager, 670 employees, public sector.

"We have a disaster site and there is alternate routing if that's taken out. The email and the network would not be affected. We would have file, print and telephony and the email would not be affected. Only external email would be affected. We would lose our data process application thought. (Researcher - How long would that take to restore?) That is not part of our skeleton operations. That would not be affected." (Researcher - What about getting things mostly back up and running?) The data application would take 2-10 days. (Researcher - And what about achieving 100% normal operations again?) We are looking at 15 working days." UK, IT Manager, 2,500 employees, public sector.

"We would expect within a day or two we'd restore critical services. (Researcher - What about getting things mostly back up and running?) I don't have a figure - probably weeks. It could be 1 or 2 weeks. (Researcher - And what about achieving 100% normal operations again?) I suspect that would be a month. There are some assumptions made here in terms of insurance and suppliers. (Researcher - How is that?) Assuming insurance goes to plan and suppliers too." UK, IT Manager, 600 employees, public sector.

"We need 2 days for skeleton operations, and about 1 week for 100% normal operations." Germany, IT Manager, 800 employees, public sector.

"For skeleton operations, it takes 2-3 days. (Researcher - And what about achieving 100% normal operations again?) About 3 weeks." Jordan, IT Manager, 2,000 employees, public sector.

"We would need about 2-3 days to have basic operations. To get it all up and running we would need 7 days." Russia, IT Director, 2,330 employees, power and energy sector.

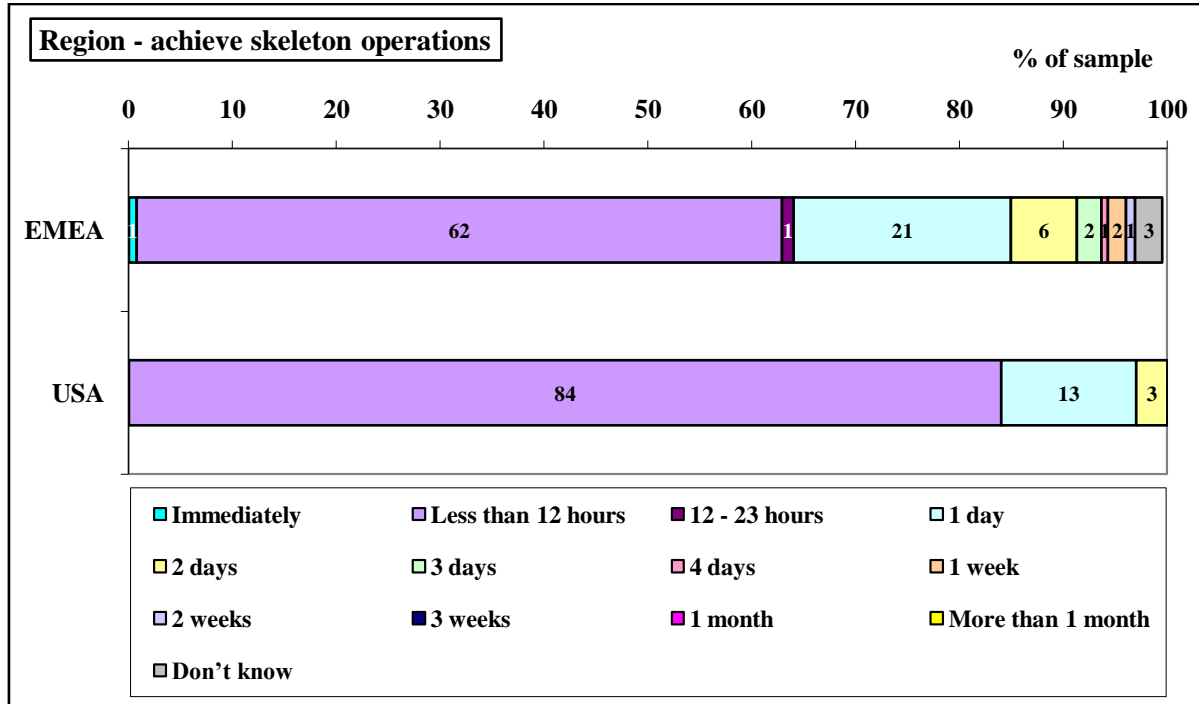
"We need 1 week for the skeleton operations. (Researcher - And what about achieving 100% normal operations again?) That would be about 1 month for 100% operations." USA, IT Manager, 900 employees, public sector.

"To reinstate skeleton operations we would need 1 month. To reinstate 100% normal operations, we would need 3 months." Italy, IT Director, 550 employees, public sector.

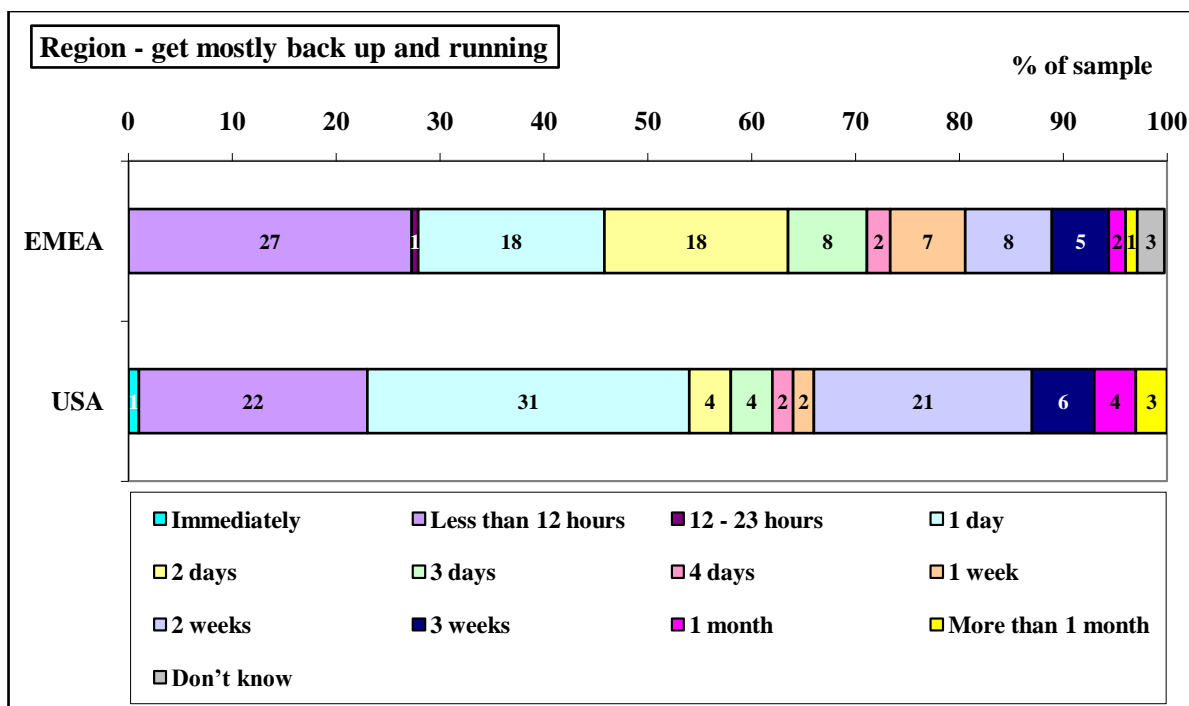
"To reinstate skeleton operations, we would need 2 months. (Researcher - And what about achieving 100% normal operations again?) That would take 3 months." Italy, IT Director, 540 employees, public sector.

Table 18: Average time needed to recover from a major fire disaster: regions

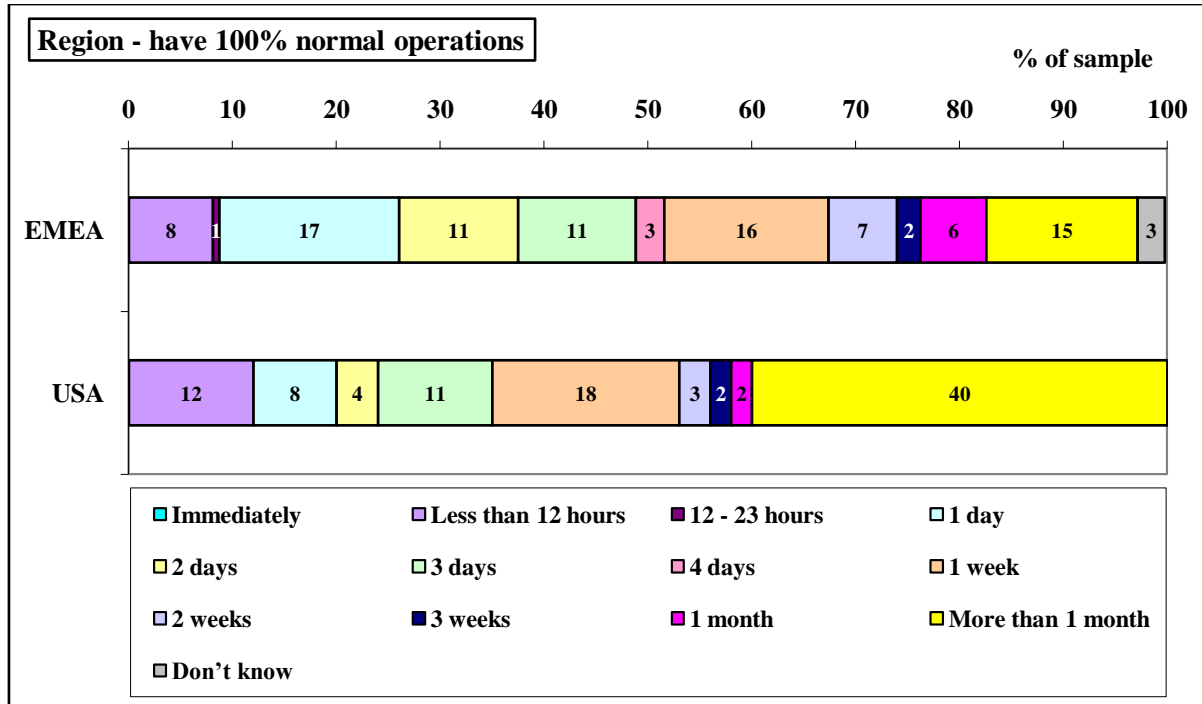
Region	Achieve skeleton operations	Get mostly back up and running	Have 100% normal operations
EMEA	0.8 days	4.9 days	17.5 days
USA	0.3 days	7.8 days	30.6 days



- On average, EMEA organisations think it would take more time (0.8 days) for them to establish skeleton operations following a major fire disaster, compared to US organisations (0.3 days).
- Also, more EMEA organisations (21%) say they could achieve skeleton operations in 1 day or 24 hours, compared to US organisations (13%).
- But, more US organisations (84%) say they could achieve skeleton operations within less than 12 hours, compared to EMEA organisations (62%).



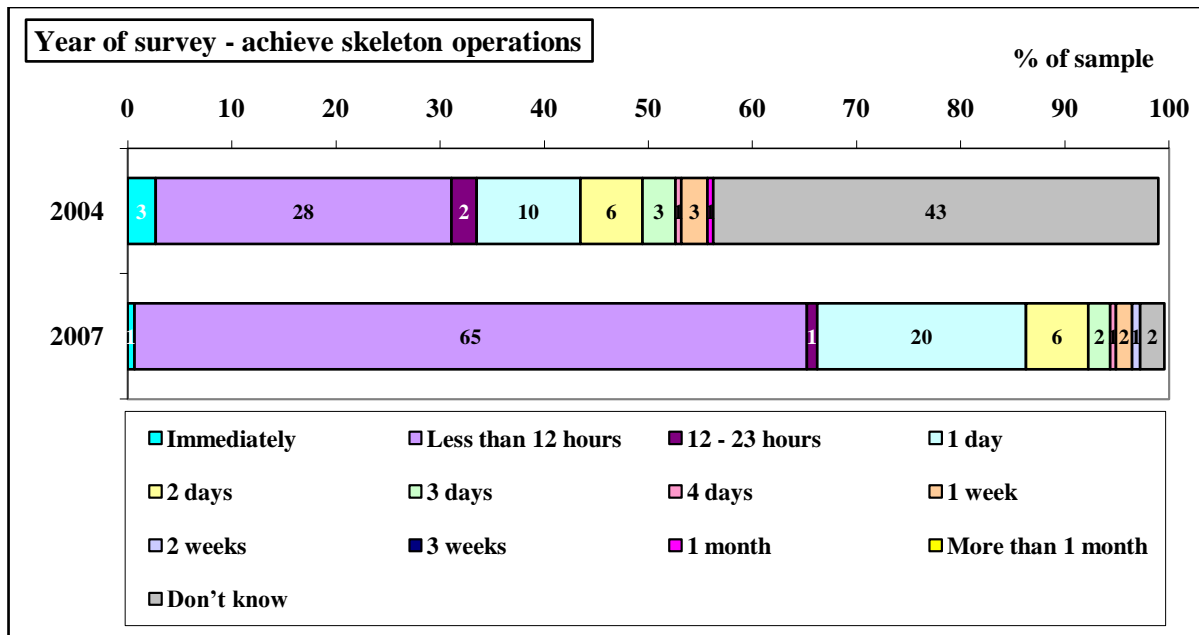
- On average, US organisations think it would take more time (7.8 days) for them to get mostly back up and running following a major fire disaster, compared to EMEA organisations (4.9 days).
- However, more US organisations (31%) say they could get mostly back up and running in 1 day or 24 hours, compared to EMEA organisations (18%).
- But, more EMEA organisations (18%) say they could achieve this status in 2 days, compared to US organisations (4%).
- Also, more EMEA organisations (7%) say they could get mostly back up and running in 1 week, compared to US organisations (2%).
- Whereas, more US organisations (21%) say they could get mostly back up and running in 2 weeks, compared to EMEA organisations (8%).



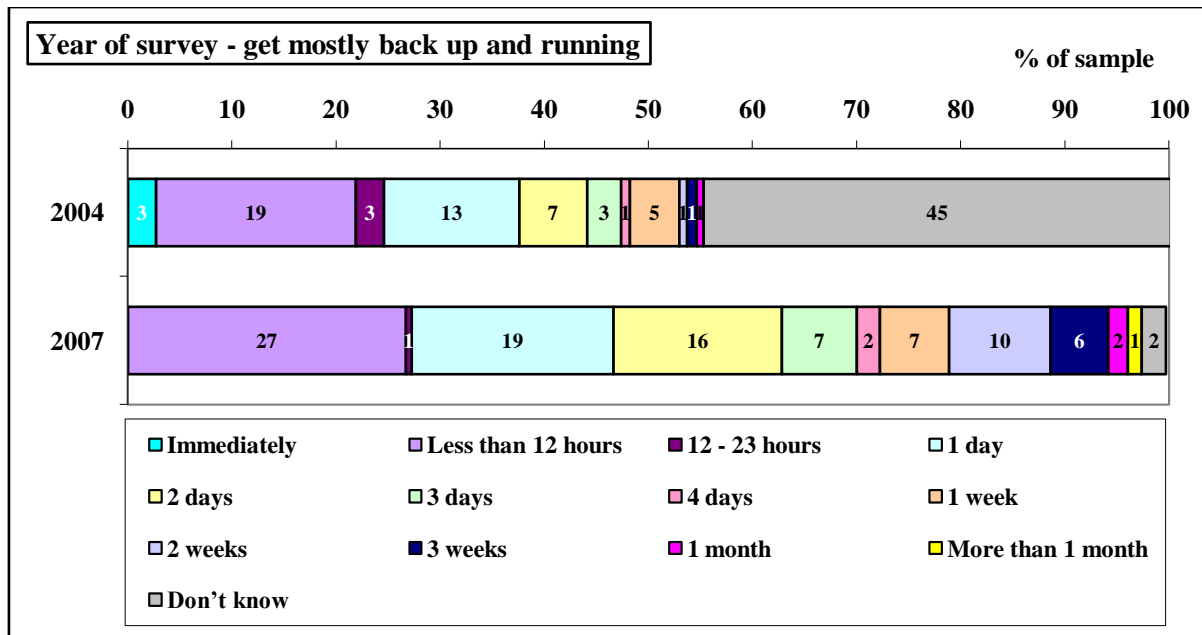
- On average, US organisations think it would take more time (30.6 days) for them to get back to 100% normal operations following a major fire disaster, compared to EMEA organisations (17.5 days).
- And, more US organisations (65%) say they could get back to 100% normal operations in 1 week or longer, compared to EMEA organisations (46%).
- But, more EMEA organisations (17%) say they could get back to normal in 1 day or 24 hours, compared to US organisations (8%).
- And, more EMEA organisations (11%) say they could get back to normal in 2 days, compared to US organisations (4%).
- Whereas, more US organisations (40%) say they could get back to 100% normal operations in more than 1 month, compared to EMEA organisations (15%).

Table 19: Average time needed to recover from a major fire disaster: year of survey

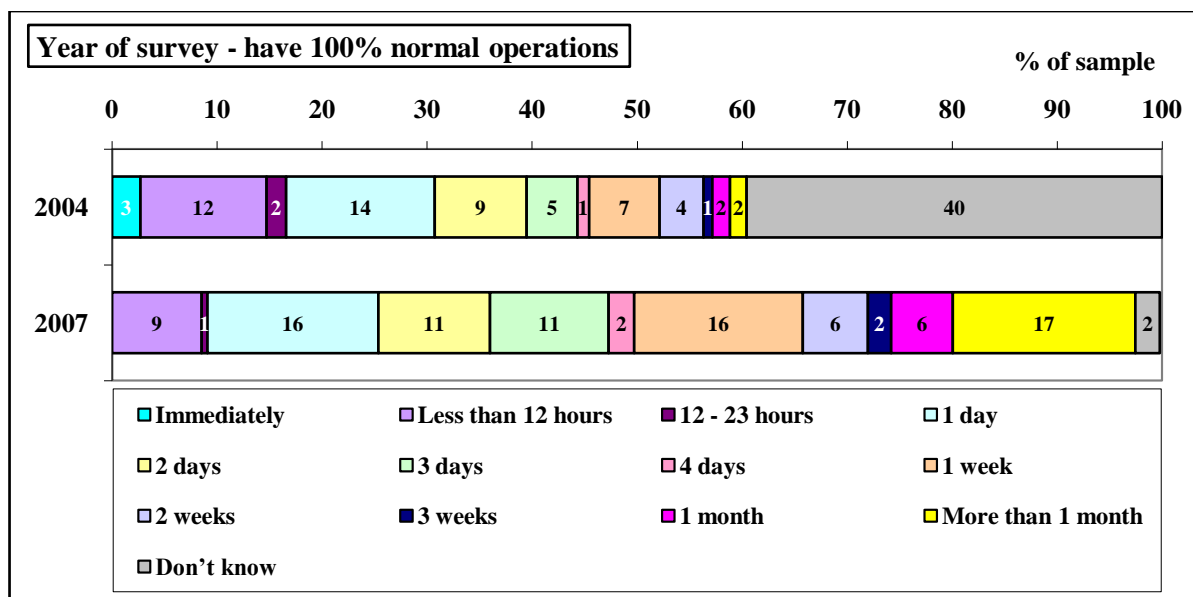
Year of survey	Achieve skeleton operations	Get mostly back up and running	Have 100% normal operations
2004	3.2 days	4 days	6.6 days
2007	0.8 days	5.3 days	19 days



- Overall, organisations questioned in 2007 say they can achieve skeleton operations in shorter time scales, compared to those questioned in 2004.
- But more organisations questioned in 2004 (3%) say they could achieve skeleton operations immediately, compared to organisations questioned in 2007 (1%) – this might reflect the reduction in the use of 3rd party organisations over this period.
- But, significantly more organisations questioned in 2007 (65%) say they could achieve skeleton operations within less than 12 hours, compared to 2004 (28%).
- Also, more organisations questioned in 2007 (20%) say they could achieve skeleton operations in 24 hours, compared to 2004 (10%).
- However, some of the above differences might be due to the fact that more organisations questioned in 2004 (43%) did not know how long it would take to achieve skeleton operations, compared to organisations questioned in 2007 (2%).



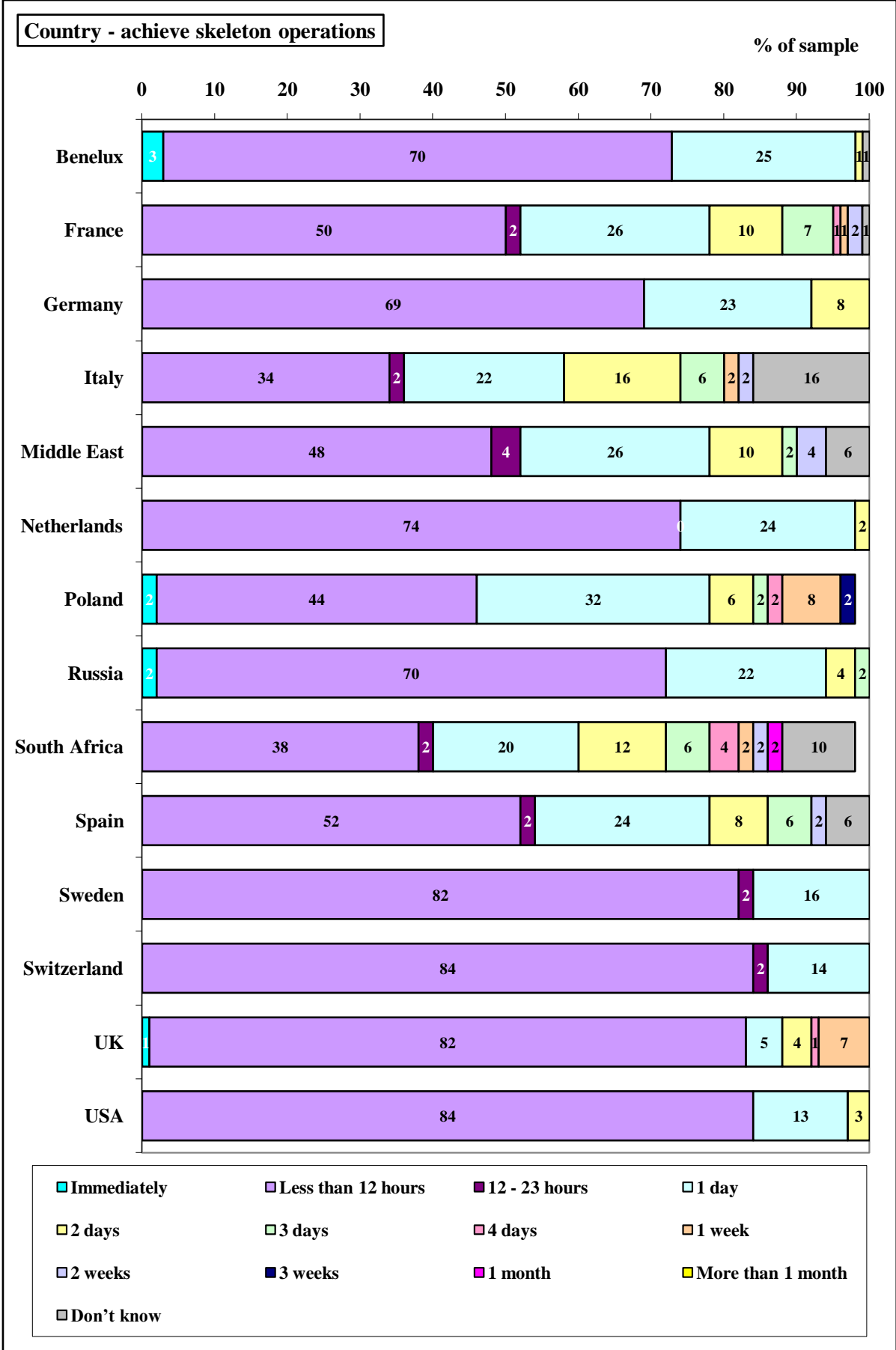
- More organisations questioned in 2007 (27%) say they could get mostly back up and running in less than 12 hours, compared to organisations questioned in 2004 (19%).
- And, more organisations questioned in 2007 (19%) say they could get mostly back up and running in 24 hours or 1 day, compared to 2004 (13%).
- Similarly, more organisations questioned in 2007 (16%) say they could get mostly back up and running in 2 days, compared to 2004 (7%).
- Also, more organisations questioned in 2007 (7%) say they could get mostly back up and running in 3 days, compared to 2004 (3%).
- In addition, more organisations questioned in 2007 (10%) say they could get mostly back up and running in 2 weeks, compared to 2004 (1%).
- Furthermore, more organisations questioned in 2007 (6%) say they could get mostly back up and running in 3 weeks, compared to 2004 (1%).
- However, some of the above differences will be due to the fact that more organisations questioned in 2004 (45%) did not know how long it would take them to get mostly back up and running, compared to organisations questioned in 2007 (2%).

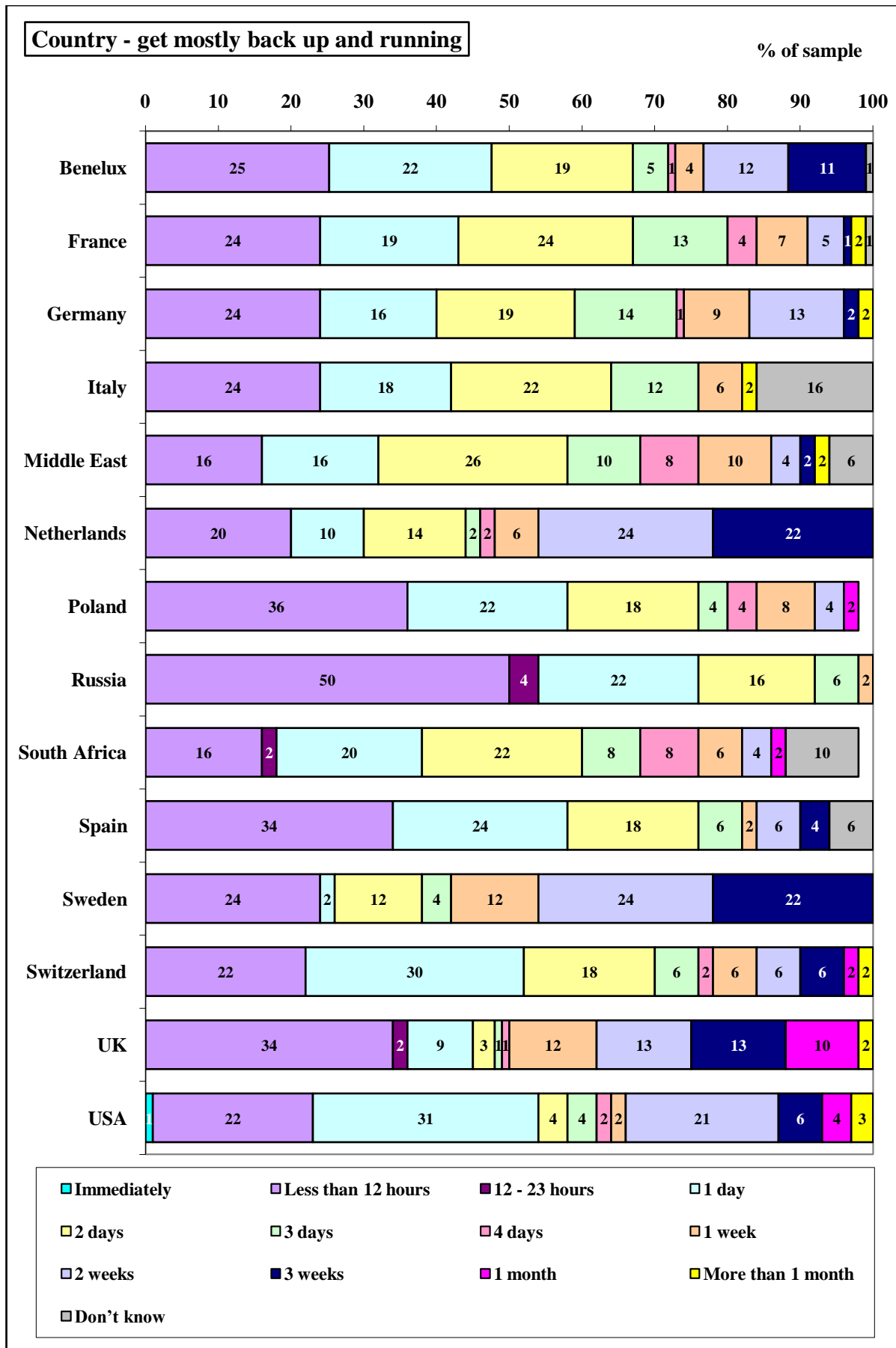


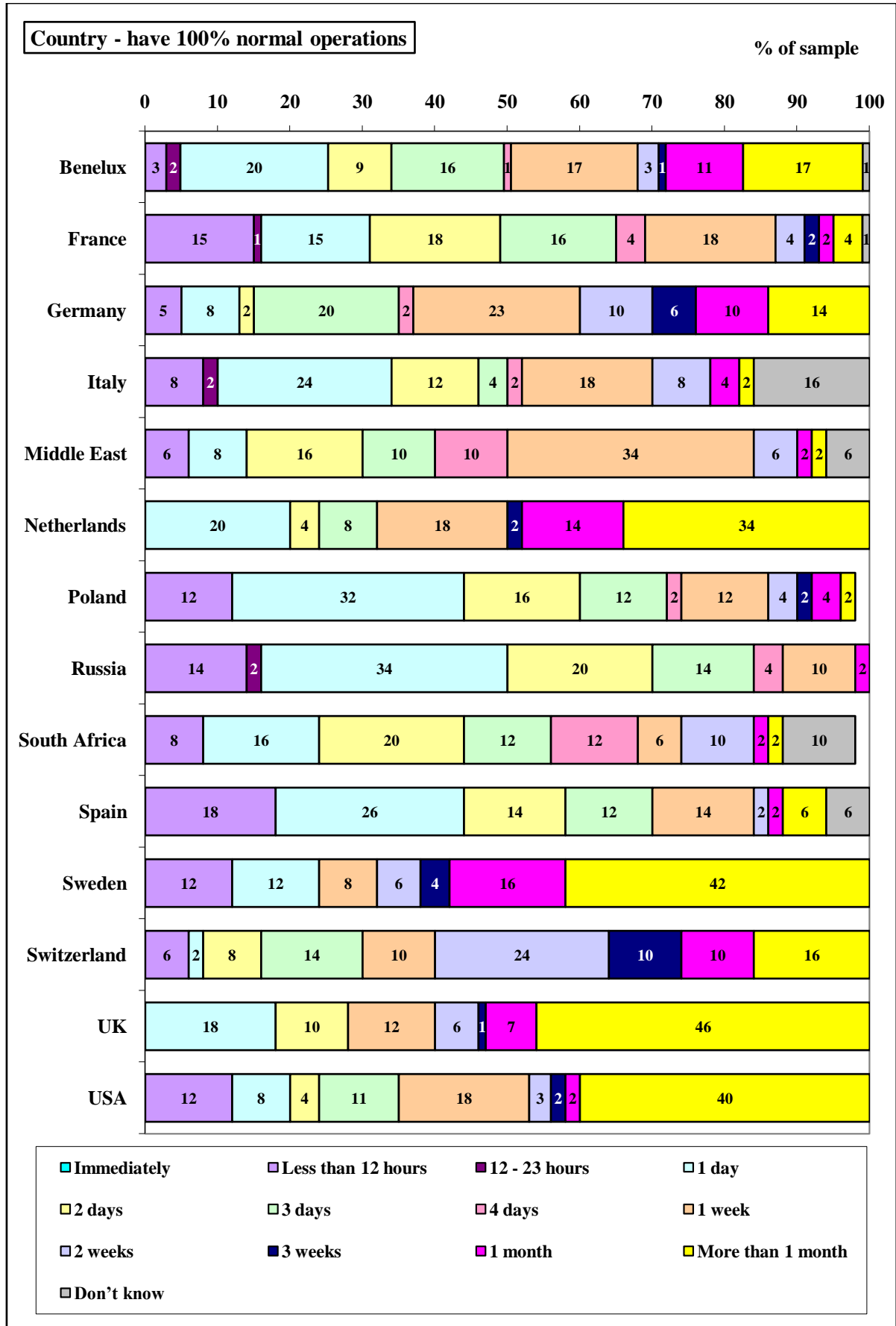
- More organisations questioned in 2004 (12%) say they could have 100% normal operations in less than 12 hours, compared to organisations questioned in 2007 (9%).
- But, more organisations questioned in 2007 (11%) say they could have 100% normal operations in 3 days, compared to 2004 (5%).
- And, more organisations questioned in 2007 (16%) say they could have normal operations in 1 week, compared to 2004 (8%).
- And, more organisations questioned in 2007 (17%) say they could have 100% normal operations in more than 1 month, compared to 2004 (2%).
- However, some of these differences might be due to the fact that more organisations questioned in 2004 (40%) did not know how long it would take them to have 100% normal operations, compared to organisations questioned in 2007 (2%).

Table 20: Average time needed to recover from a major fire disaster: countries

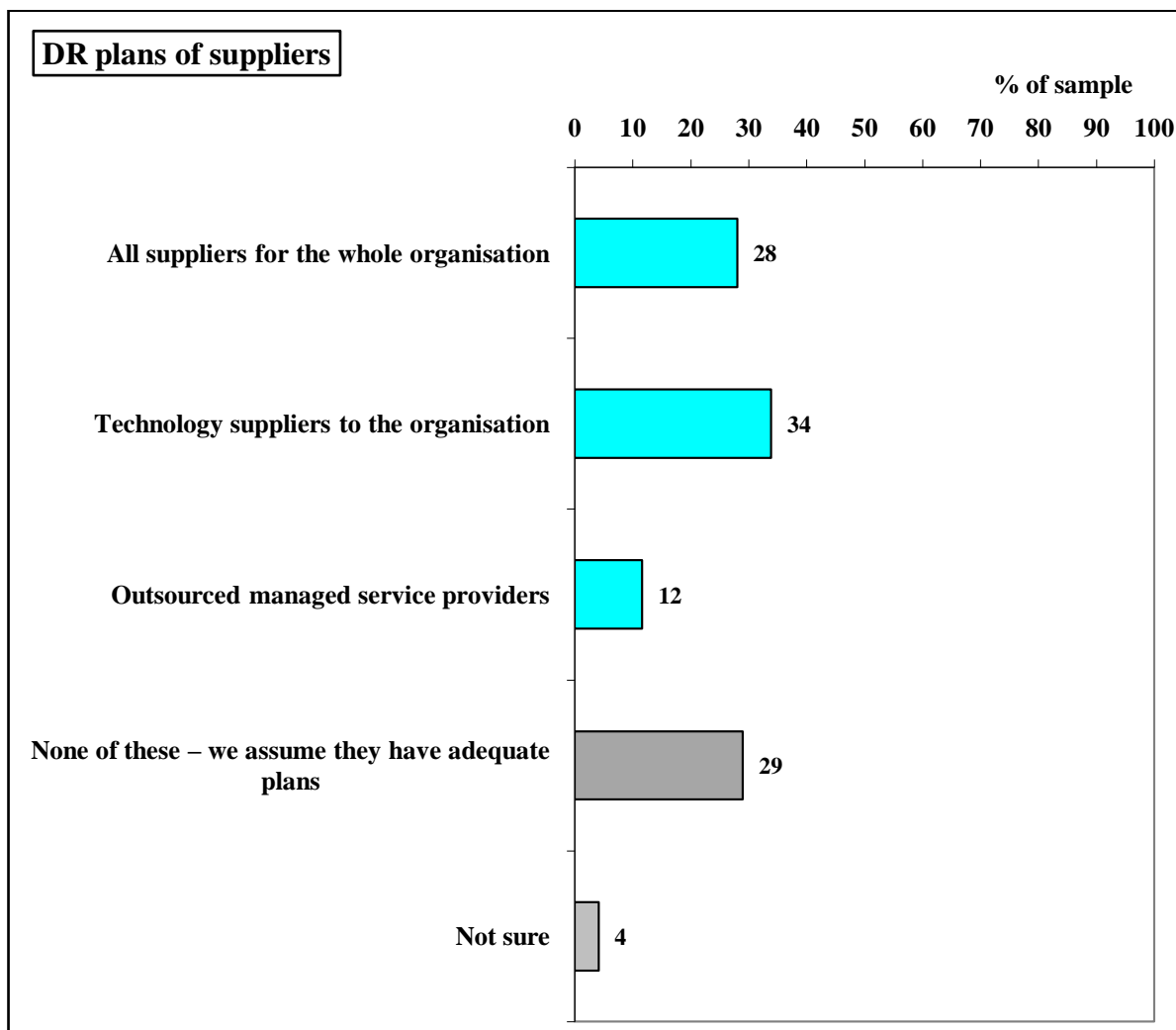
Country	Achieve skeleton operations	Get mostly back up and running	Have 100% normal operations
Benelux	0.3 days	5.0 days	16.2 days
France	1.2 days	3.9 days	8.9 days
Germany	0.4 days	5.0 days	18.3 days
Italy	1.4 days	2.7 days	6.0 days
Middle East	1.3 days	4.1 days	5.9 days
Netherlands	0.4 days	8.8 days	27.5 days
Poland	1.6 days	2.7 days	5.3 days
Russia	0.4 days	1.0 days	2.7 days
South Africa	2.1 days	3.2 days	5.7 days
Spain	1.0 days	2.8 days	7.0 days
Sweden	0.3 days	9.1 days	33.9 days
Switzerland	0.2 days	4.7 days	19.3 days
UK	0.7 days	10.1 days	51.6 days
USA	0.3 days	7.8 days	30.6 days



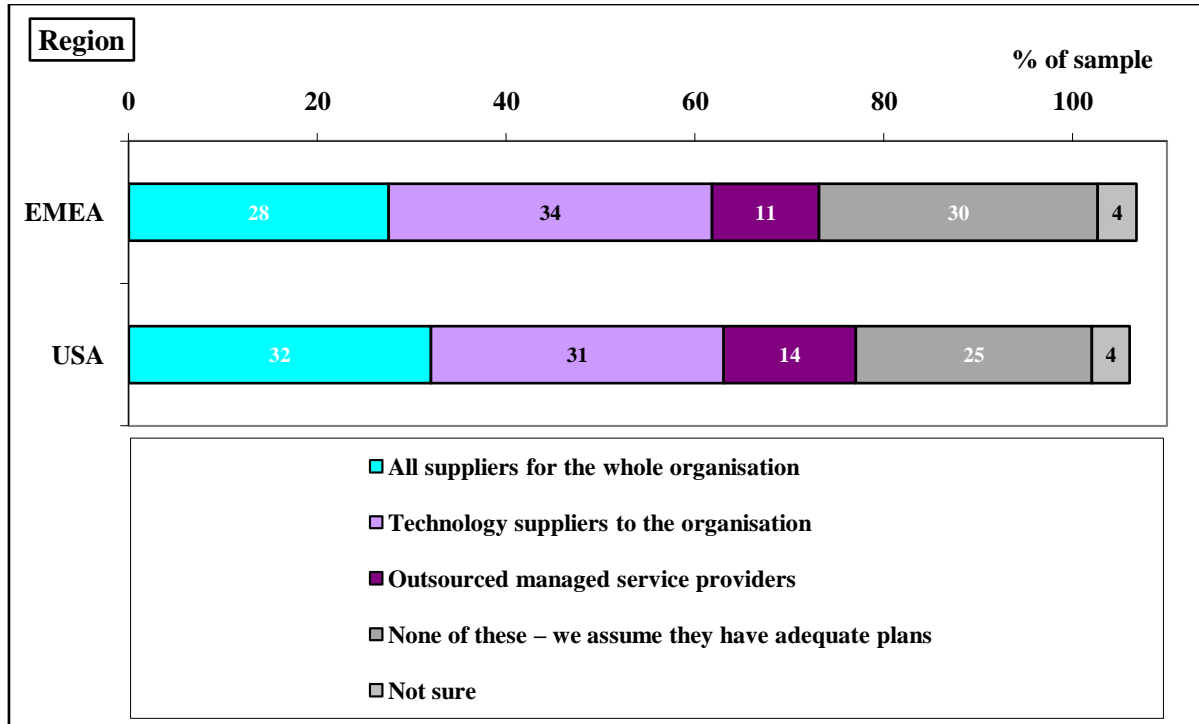




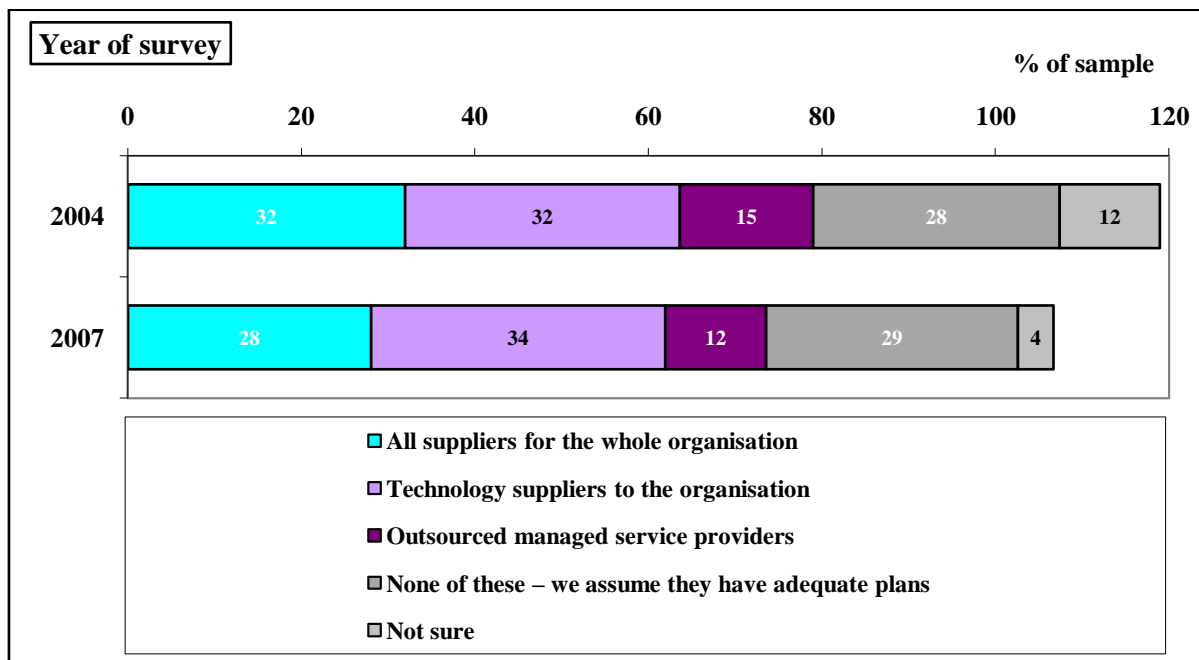
3.19 When it comes to the DR plans of suppliers to your organisation, which of the following supplier types do you routinely ask to see their business continuity and DR plans before you start work with them?



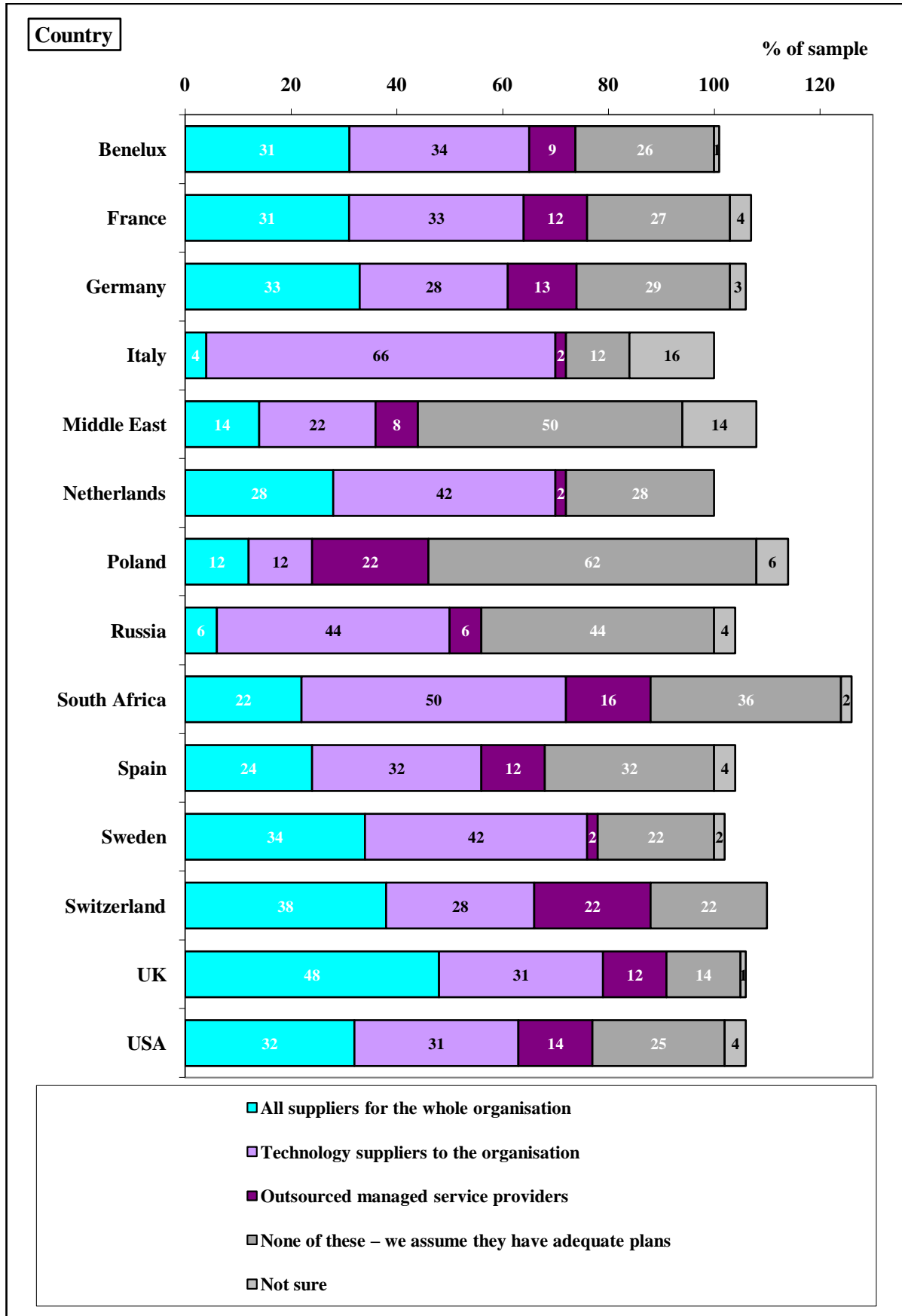
- 29% of organisations do not ask to see the BC and DR plans of any of their third party suppliers as they assume they have adequate plans.
- Another 4% are unsure about the degree to which the BC and DR plans of suppliers are given consideration by their organisation.
- Only 28% of organisations routinely ask to see the BC and DR plans of all suppliers for the whole of their organisation before they start work with them.
- Another 34% routinely ask technology suppliers this question, and 12% ask it to outsourced managed service providers.



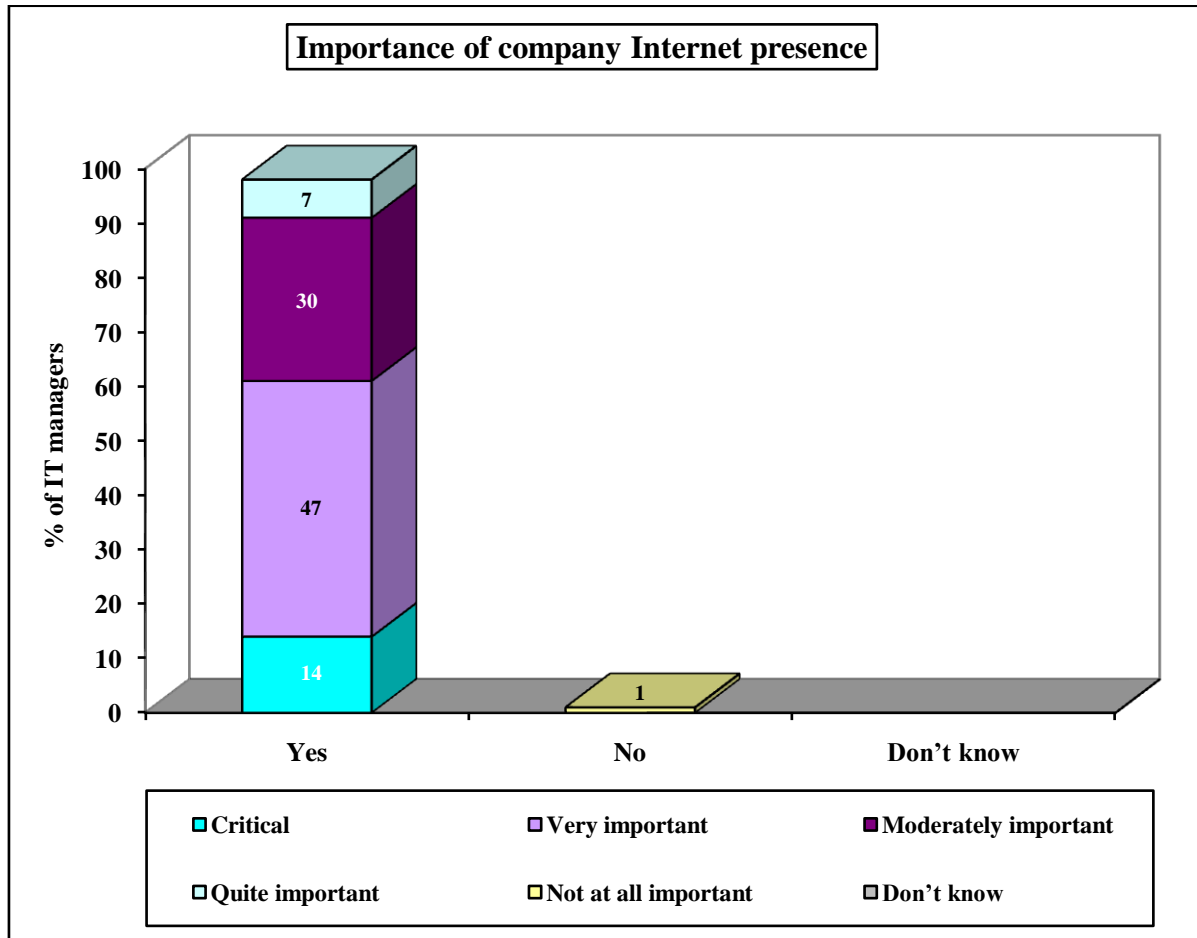
- Statistically, there is no significant difference according to region and which supplier types are routinely asked about their BC and DR plans.



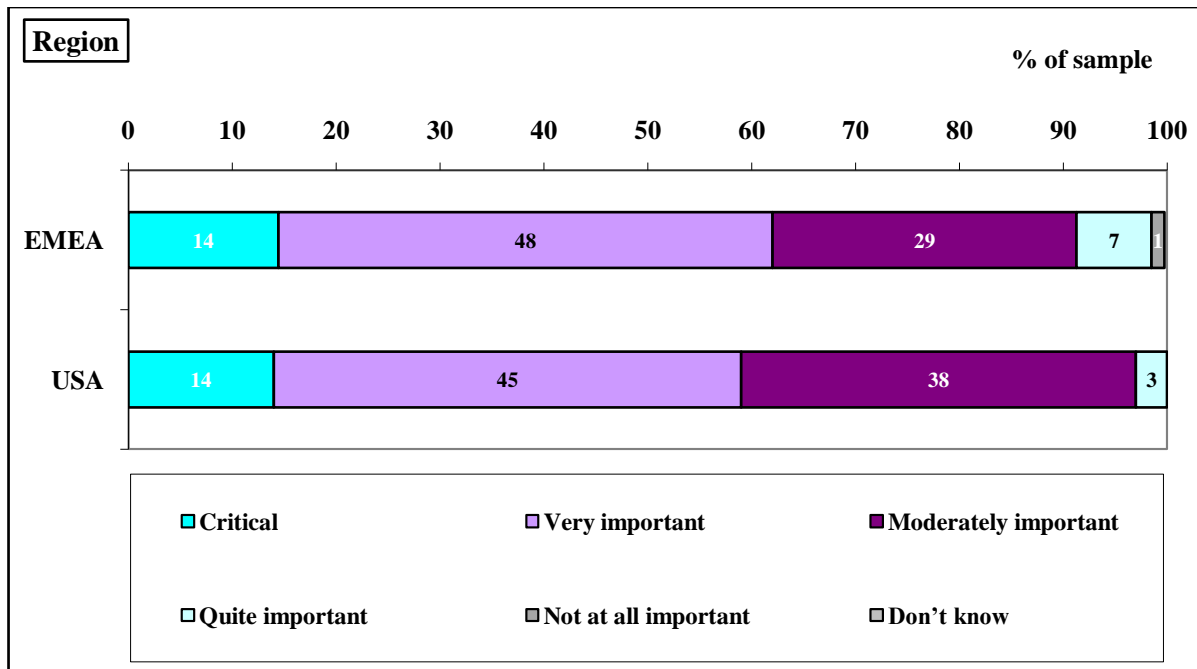
- More organisations questioned in 2004 (15%) routinely ask to see the BC and DR plans of outsourced managed service providers, compared to organisations questioned in 2007 (12%).
- But, more organisations questioned in 2004 (12%) are unsure about the degree to which the BC and DR plans of suppliers are given consideration by their organisation, compared to organisations questioned in 2007 (4%).



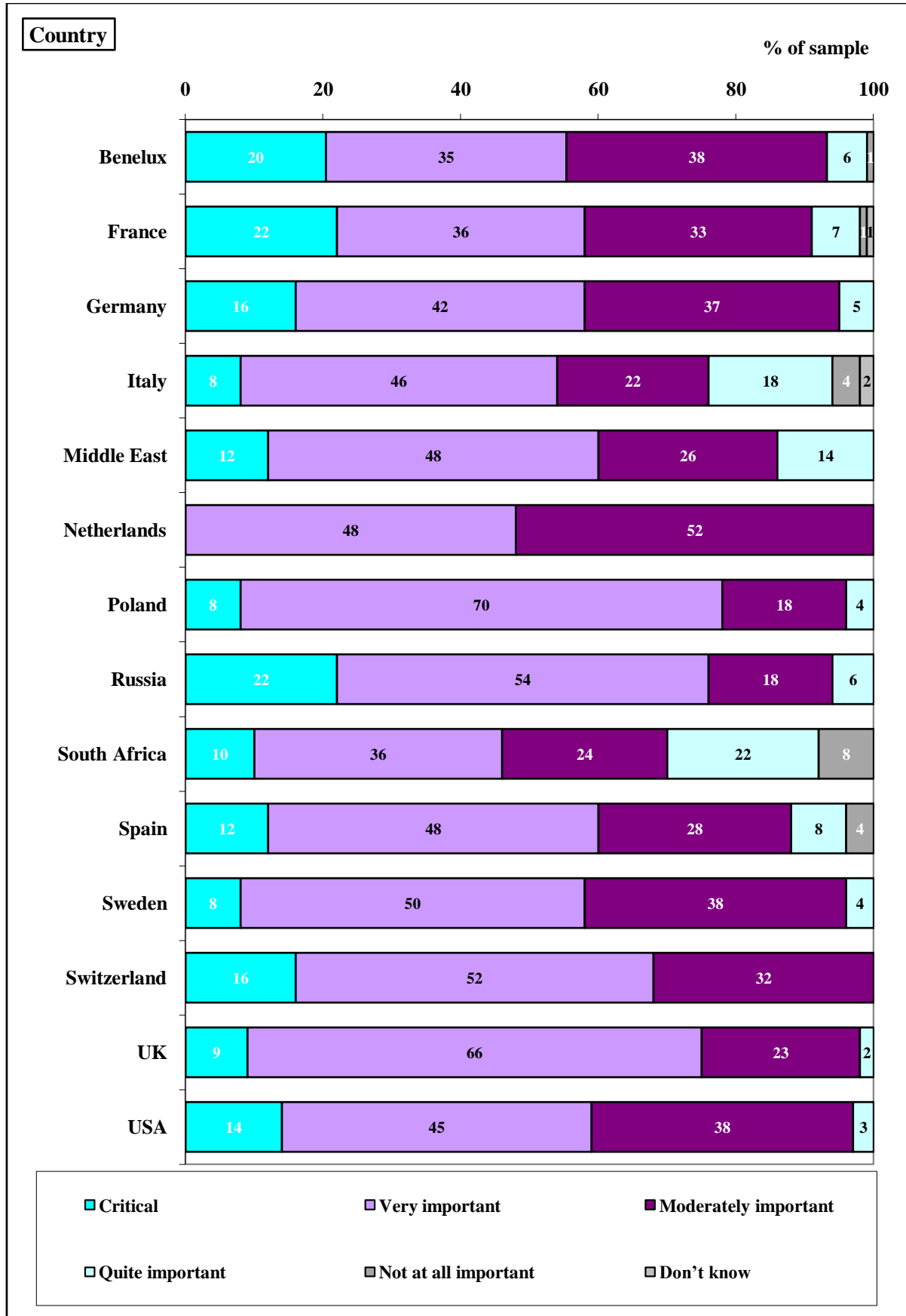
3.20 How important is your organisation’s Internet presence to its overall success?



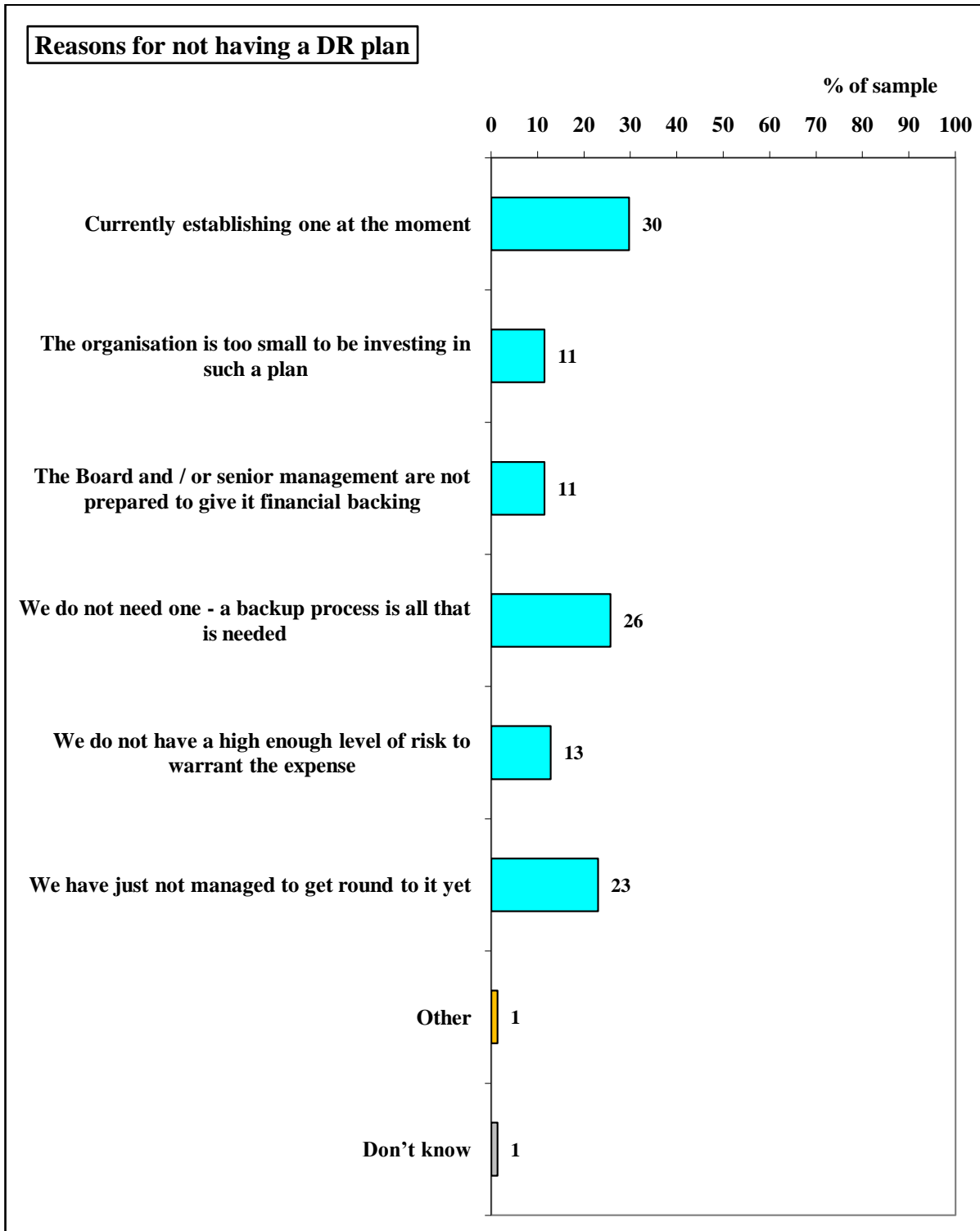
- Collectively, 99% of organisations think their Internet presence is important to some degree or other to their overall business success.
- In detail, 61% describe it as either critical (14%) or very important (47%) to their overall success.
- Yet 30% describe it as moderately important, and 7% say it is only quite important.
- Only 1% of organisations say their Internet presence is not at all important to their overall success.
- Among those who think the Internet is either critical or very important to the success of their business, only 30% say poor application performance would lead to them invoking the DR plan – 64% say it would not [not shown].



- Statistically, there is no significant difference according to region and how important an organisation's Internet presence is deemed to be to its overall business success.

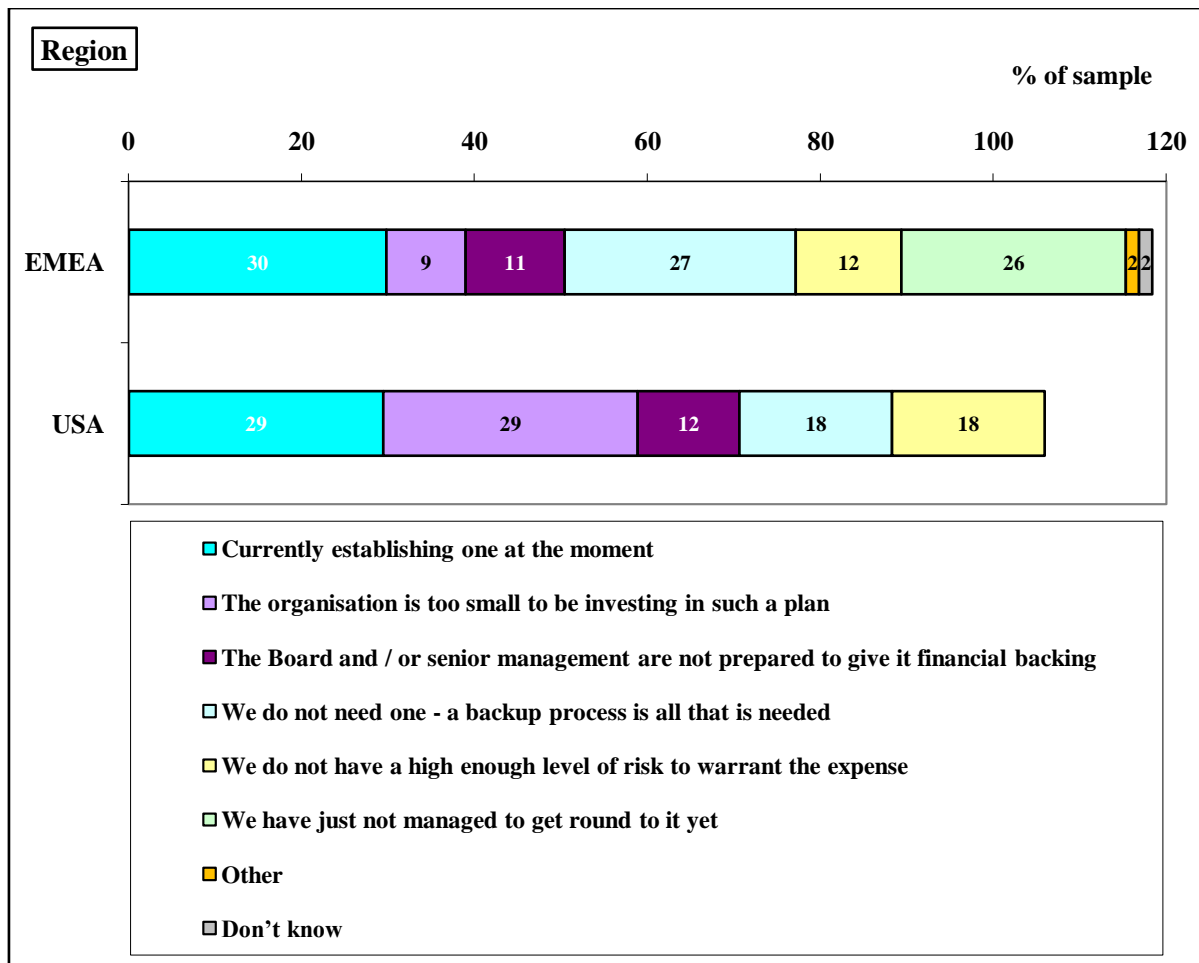


3.21 [Only to organisations without a DR plan] Which of the following applies to why you do not have a disaster recovery plan?

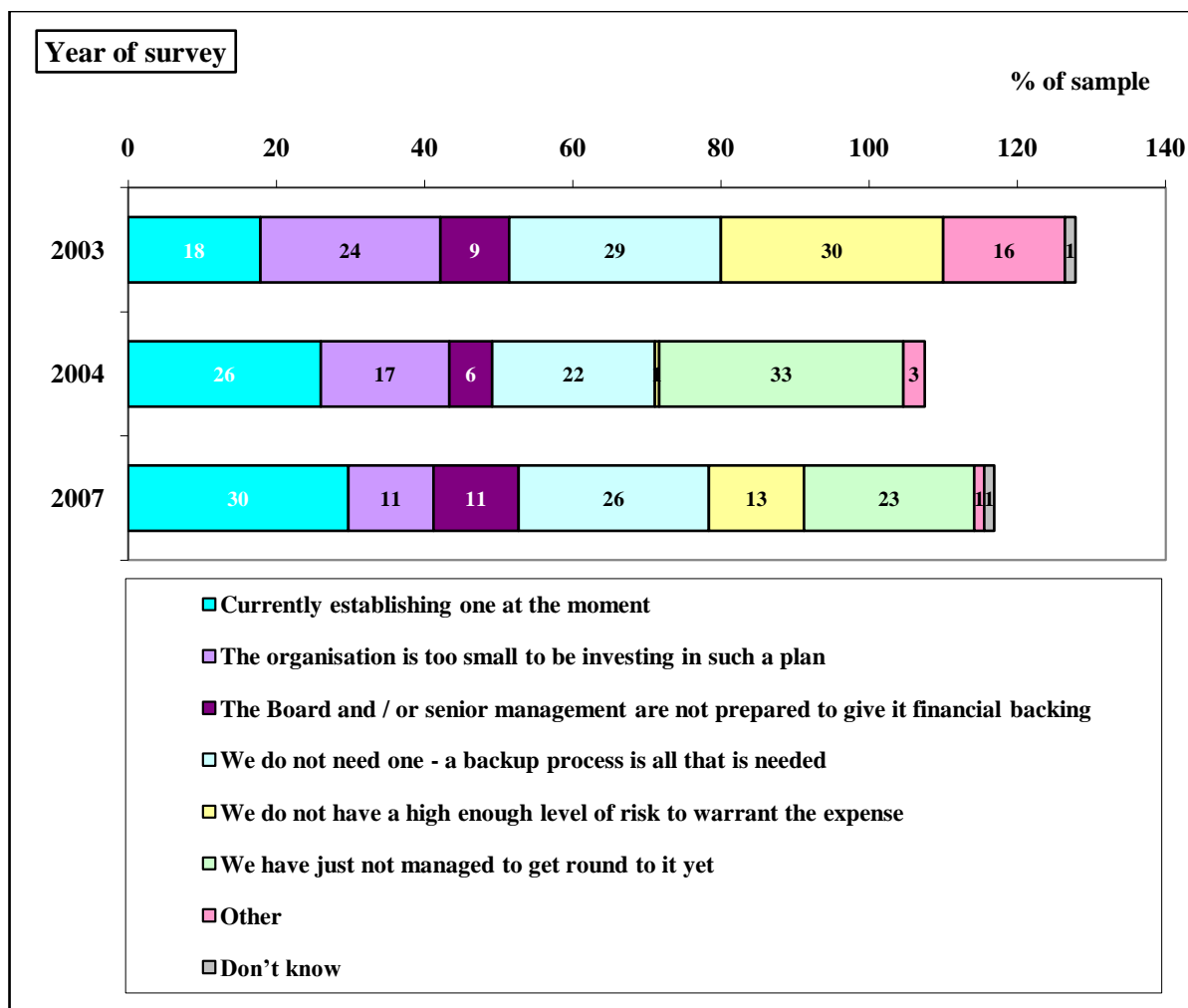


- Among organisations that do not have a DR plan, the largest proportion (30%) are currently establishing one at the moment.
- In contrast, 26% think they do not need a DR plan and think a backup process is all that is needed.

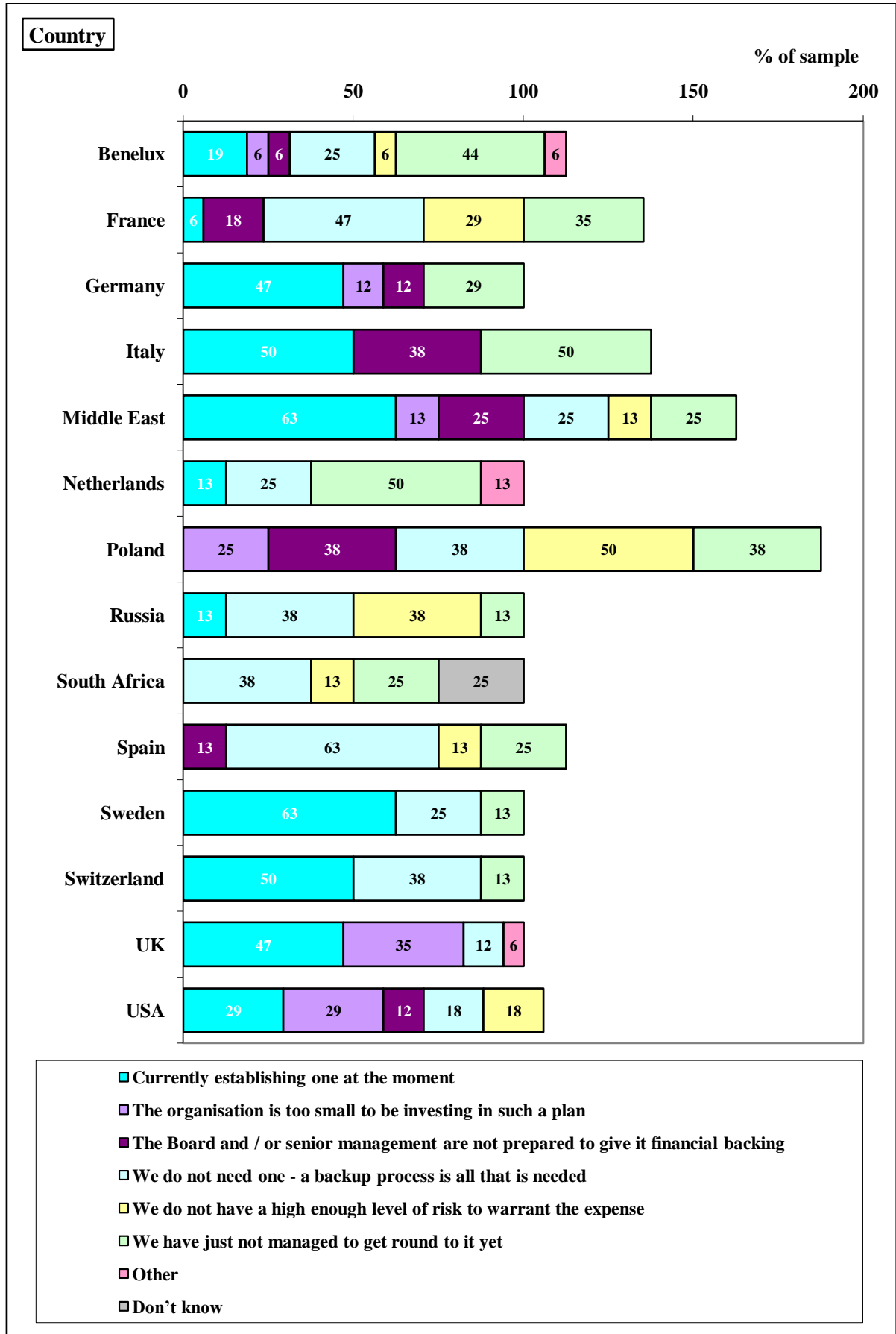
- But another 23% say they have just not managed to get round to it yet.
- 13% think they do not have a high enough level of risk to warrant the expense.
- And 11% say their organisation is too small to be investing in such a plan.
- Another 11% say the Board and / or senior management are not prepared to give it financial backing.
- The ‘other’ category includes:
 - IT is outsourced.
- Another 1% are not sure why their organisation does not have a disaster recovery plan.



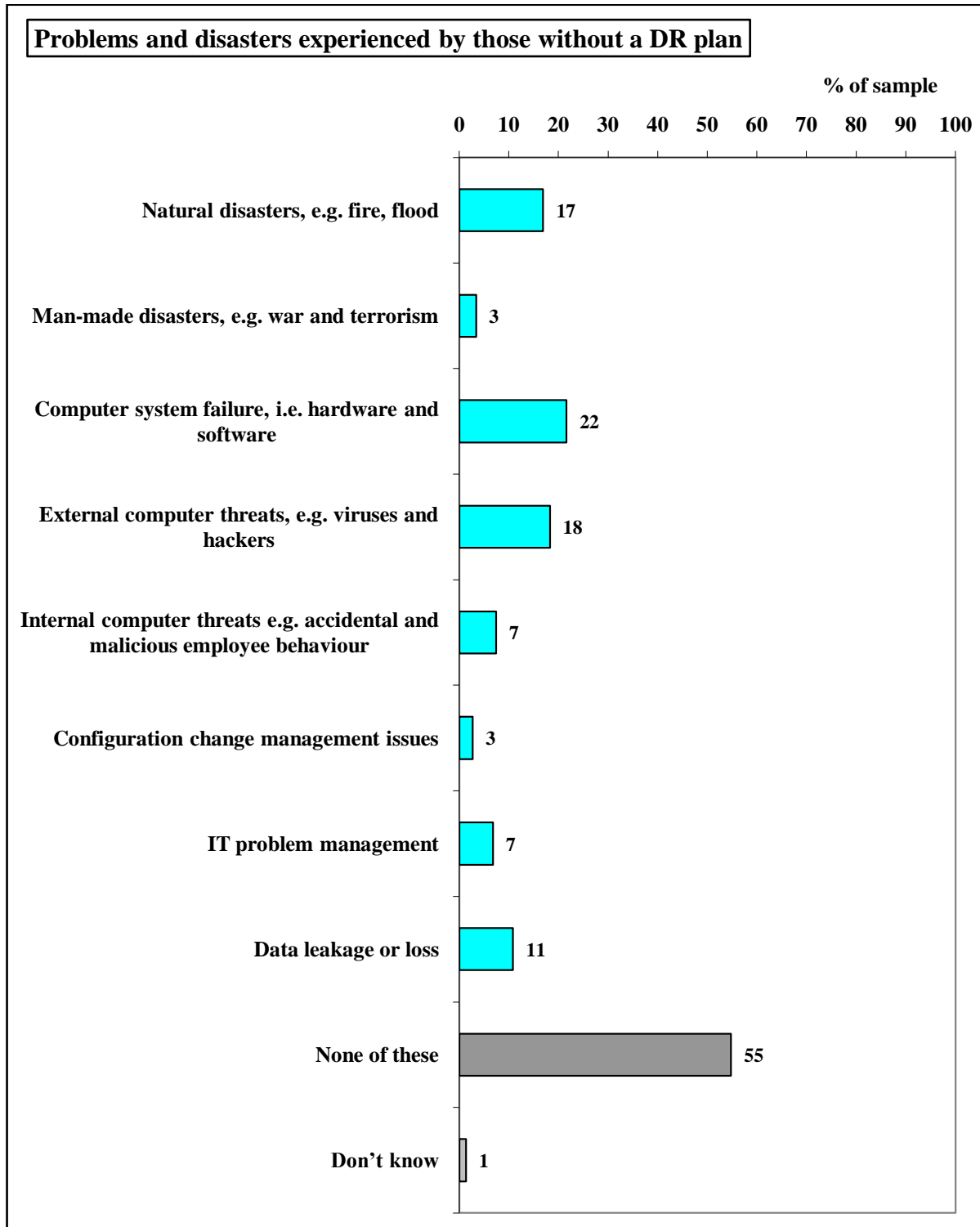
- Statistically, there is no significant difference according to region and the reasons why organisations do not have a DR plan.



- More organisations questioned in 2007 (30%) say they do not have a DR plan because they are establishing one at the moment, compared to organisations questioned in 2003 (18%).
- But, more organisations questioned in 2003 (24%) say they do not have a DR plan because they are too small to be investing in such a plan, compared to organisations questioned in 2007 (11%).
- And, more organisations questioned in 2003 (30%) say they do not have a DR plan because they do not have a high enough level of risk to warrant the expense, compared to organisations questioned in 2004 (1%) and 2007 (13%).
- In contrast, more organisations questioned in 2004 (33%) said they did not have a DR plan because they have just not managed to get round to it yet, compared to organisations questioned in 2007 (23%).

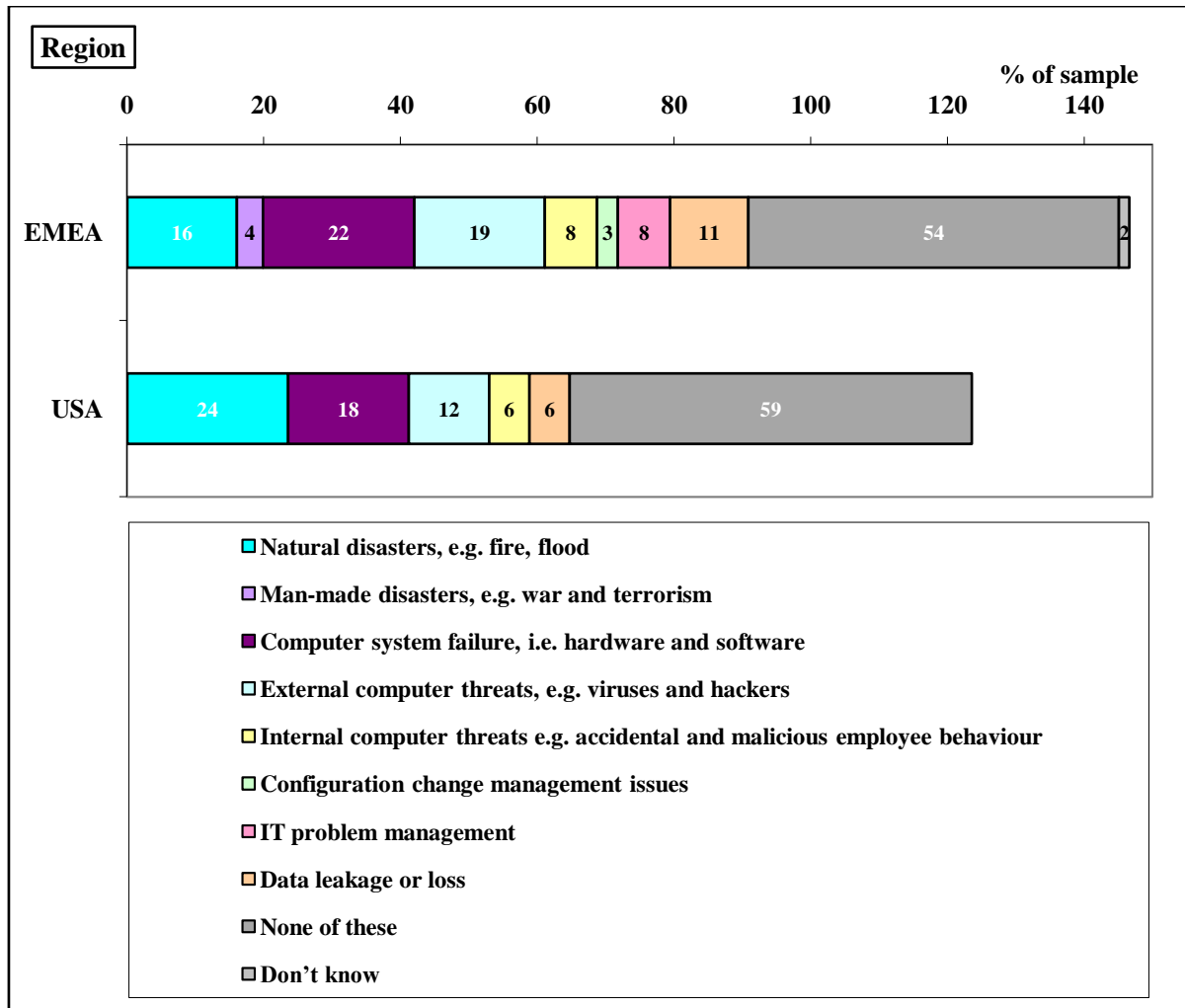


3.22 [Only to organisations without a DR plan] Which of the following has your organisation ever experienced?

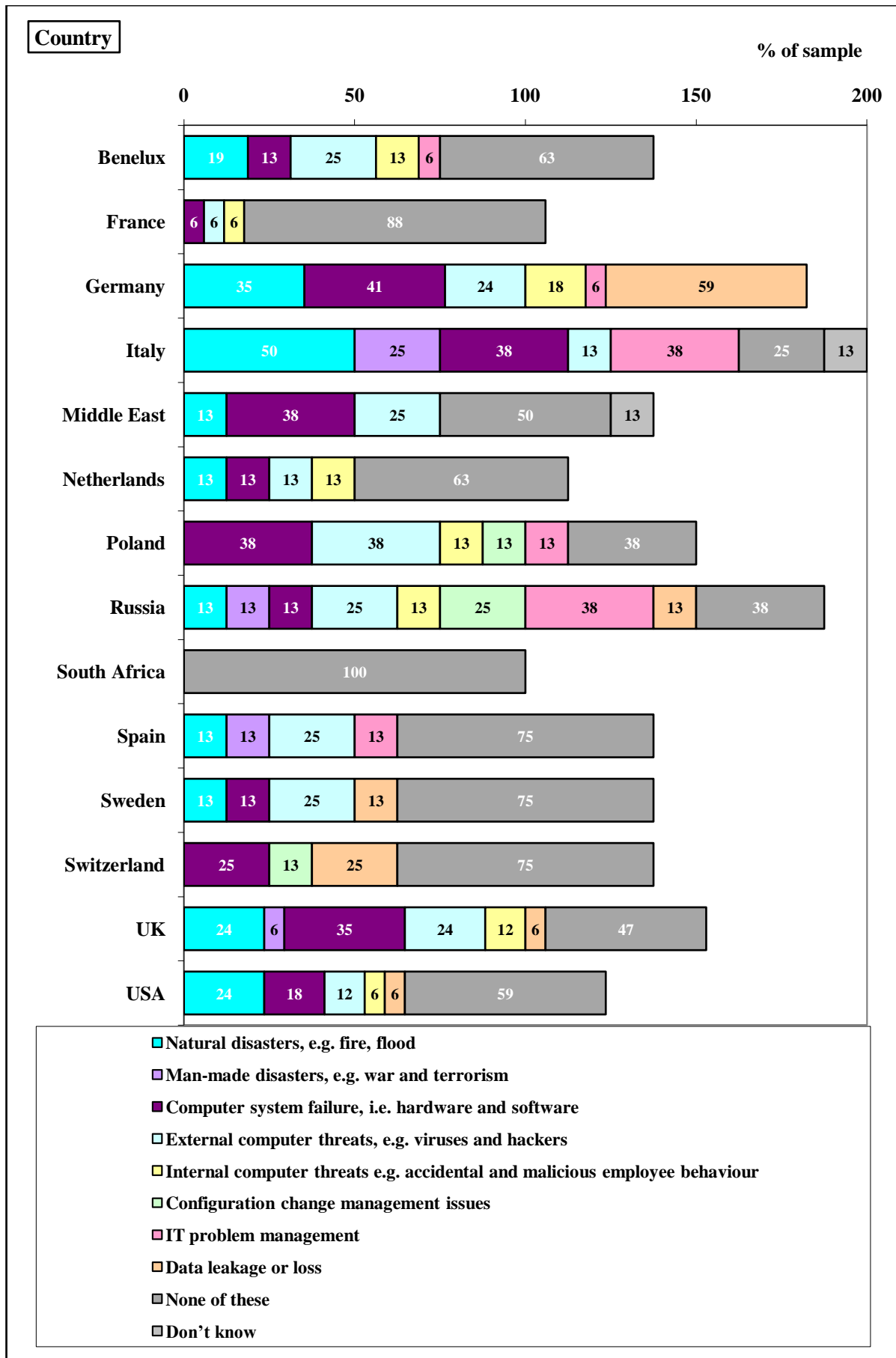


- Collectively, 44% of organisations without a DR plan have experienced at least 1 of these types of problems or disasters.
- Indeed, 26% have experienced 2 or more and 11% have experienced 3 or more [not shown].

- The Top 3 disasters experienced by those without a DR plan are:
 1. Computer system failure (22%)
 2. External computer threats from viruses and hackers (18%)
 3. Natural disasters like fire and floods (17%)
- 11% have had data leakage or loss, 7% have seen accidental or malicious employee behaviour and the same amount have suffered from IT problem management (7%).
- Just 3% have been affected by man-made disasters, like war and terrorism, and the same amount (3%) have suffered from configuration change management issues.
- In contrast, 55% of those without a DR plan say their organisation has not experienced any of these, and another 1% are unsure.



- Statistically, there is no significant difference according to region and which of these threats or disasters the organisations have experienced.



Appendix A: Quantitative Questionnaire

Qualifying Questions:

A. Does your organisation have at least 500 employees worldwide? [Select only 1]

- Yes [Continue]
- No [Terminate the interview]

Bi. Does your organisation have a disaster recovery plan? [Select only 1]

- Yes [Continue to Qu C]
- No [ask Qu Bii and Biii and then terminate the interview]

Bii. Which of the following applies to why you do not have a disaster recovery plan? [Select all that apply]

- Currently establishing one at the moment
- The organisation is too small to be investing in such a plan
- The Board and / or senior management are not prepared to give it financial backing
- We do not need one - a backup process is all that is needed
- We do not have a high enough level of risk to warrant the expense
- We have just not managed to get round to it yet
- Other (please specify)
- [Don't know]

Biii. Which of the following has your organisation ever experienced? [Select all that apply]

- Same list as Qu 14 (i.e. the list of threats)

C. Are you responsible for the organisation's disaster recovery plan and are you involved in the day-to-day management of the plan?

- Yes [Continue]
- No [Ask who is and then terminate the interview]

Introduction by researcher:

In this questionnaire, we refer to disaster recovery plans and business continuity plans. By business continuity we mean a plan that will restore and maintain the overall operations of the organisation in the event of a disaster, whereas by disaster recovery plan, we mean a plan that will restore and maintain the IT systems of the organisation.

Main Questions:

1. Which of the following prompted your organisation to first create a disaster recovery strategy and plan? [Select all that apply]

- Natural disasters
- War and / or terrorism
- Virus attacks
- Accidental or malicious employee behaviour
- Appointment of a senior IT person
- Appointment of a senior non-IT person
- Government and industry sector regulations
- Insurance policy
- Pressure from customers, suppliers and the competition
- Changes in technology infrastructure
- Increased number of people working from home
- Increased use of mobile technology
- Increase in patches
- Increased concern over data loss, such as customer names / order details etc.
- [None of these]
- [Don't know]

2. In which of the following ways does your business continuity plan relate to your disaster recovery plan? [Select only 1]

- Both exist as separate plans
- Both exist and are integrated
- Only the DR plan exists – there is no business continuity plan
- We do not differentiate between disaster recover and business continuity
- Not sure

3. Where is the disaster recovery plan located? [Select all that apply]

- At the organisation’s main data centre
- At another of our buildings away from the main data centre [at the end of the question, ask how many kilometres that is from your main data centre]
- Off-site at a 3rd party’s secure location [at the end of the question, ask how many kilometres that is from your main data centre]
- Off-site in an ad-hoc location, e.g. employee’s home, car or laptop
- [Don’t know]

4. On which of the following media is the DR plan located? [Select all that apply]

- Paper-based file
- On an Intranet site
- On an Internet site
- As a file on the network
- As a file on a laptop
- On a USB device or similar
- Other (pilot only)
- [Don’t know]

5. Which of the following people are on your organisation’s DR committee? [Select all that apply]

- Divisional / departmental IT manager
- Systems / infrastructure manager
- CIO / CTO / IT director
- Chief security officer
- CFO
- Line of business heads
- Other directors
- CEO
- Non-IT senior managers
- External consultancy
- None – we do not have a DR committee
- [Don’t know]

6. If your organisation were to fall on hard economic times tomorrow, which of the following would apply to the investment in your organisation’s DR plan? [Select only 1]

- All ongoing investment would be frozen and all activity would be put on hold
- Investment would be reduced but it would still carry on
- All ongoing investment would be maintained and safeguarded
- Investment would be increased, if deemed necessary
- Not sure

7. Which of the following technology types do you have and which are covered by the DR plan? [Select all that apply]

	Have in organisation	Covered by DR plan
Database servers		
Applications		
Email		
Web servers		
Desktop environment		
Laptop environment		
Mobile technology such as handheld devices		
Remote offices		

Home workers' PCs		
-------------------	--	--

- [None of these]
- [Don't know]

8. How frequently does your organisation carry out full scenario testing of its disaster recovery plan, involving relevant people, processes and technologies? [Select only 1]

- Monthly
- Every 3 months
- Every 6 months
- Once a year
- Every 1-2 years
- Every 2-3 years
- Less frequently than every 3 years
- On an ad-hoc basis
- Never
- [Don't know]

9. Which of the following reasons accounts for why full scenario tests have failed? [Select all that apply]

- Processes turn out to be inappropriate
- People do not do as they are supposed to
- Technology does not do what it is supposed to
- Discovery that the plan has become out of date
- Insufficient IT infrastructure at the DR site
- Other (pilot only)
- [Our tests have not failed]
- [Don't know]

10. Which of the following do you consider to be barriers to running a full scenario test on your disaster recovery plan? [Select all that apply]

- Resources, in terms of people's time
- Resources, in terms of budget
- Disruption to employees
- Disruption to customers
- Disruption to sales and the revenue stream
- Other IT projects taking a higher priority
- Not seen as a priority by top management
- Other (please specify)
- [None]
- [Don't know]

11. Have you discussed and agreed acceptable levels of risk with the non-IT, business directors in the organisation? [Select only 1]

- Yes, for all threats
- Yes, for some threats
- No, not for any threats
- Not sure

12. What percentage of your organisation's applications does it consider to be business-critical? [Record a % or 'none' or 'don't know']

13. Would poor application performance lead to the organisation invoking its DR plan?

- Yes
- No
- [Don't know]

14. Without your DR plan, which of the following threats or disasters would your organisation consider itself exposed to? [Select all that apply]

- Natural disasters, e.g. fire, flood
- Man-made disasters, e.g. war and terrorism
- Computer system failure, i.e. hardware and software

- External computer threats e.g. viruses and hackers
 - Internal computer threats e.g. accidental and malicious employee behaviour
 - Configuration change management issues
 - IT problem management
 - Data leakage or loss
 - [None of these –skip next question]
 - [Don't know]
- 15. [Just to those exposed to threats without their DR plans] For which of these threats has your organisation carried out a probability and impact assessment? By this we mean an assessment of how likely a threat is to affect you and what the potential impact would be on the business. [Read out those selected in above question, and then select all that apply here]**
- Natural disasters, e.g. fire, flood
 - Man-made disasters, e.g. war and terrorism
 - Computer system failure, i.e. hardware and software
 - External computer threats, e.g. viruses and hackers
 - Internal computer threats, e.g. accidental and malicious employee behaviour
 - Configuration change management issues
 - IT problem management
 - Data leakage or loss
 - [None of these]
 - [Don't know]
- 16. Which of the following potential impacts or consequences that could result from a disaster is your organisation most concerned about? Please select your top 5 from the list. [Select only 5]**
- Decreased employee productivity
 - Damage to customer loyalty
 - Damage to brand reputation
 - Damage to supplier relationships
 - Damage to competitive standing in the market place
 - Data loss
 - Reduction in profits
 - Reduction in revenue
 - [None of these]
 - [Don't know]
- 17. Under what circumstances have you ever had to actually execute for real your disaster recovery plan, either in full or in part? [Select all that apply]**
- Natural disasters, e.g. fire, flood
 - Man-made disasters, e.g. war and terrorism
 - Computer system failure, i.e. hardware and software
 - External computer threats, e.g. viruses and hackers
 - Internal computer threats, e.g. accidental and malicious employee behaviour
 - Configuration change management issues
 - IT problem management
 - Data leakage or loss
 - Other (please specify)
 - Never
 - [Don't know]
- 18. If you could imagine for a moment that a significant fire disaster were to occur at your organisation that completely obliterated the main data centre, how soon would the organisation be able to do each of the following: [Record NUMERICAL time and MINS / HOURS / DAYS / WEEKS / MONTHS for each of precode]**
- Achieve skeleton operations [Record time or don't know or not relevant]
 - Get mostly back up and running [Record time or don't know or not relevant]
 - Have 100% normal operations [Record time or don't know]
 - [Operations would be able to continue as normal despite the fire disaster – ask how (pilot only)]

19. When it comes to the DR plans of suppliers to your organisation, which of the following supplier types do you routinely ask to see their business continuity and DR plans before you start work with them? [Select all that apply]

- All suppliers for the whole organisation
- Technology suppliers to the organisation
- Outsourced managed service providers
- None of these – we assume they have adequate plans
- Not sure

20. How important is your organisation's Internet presence to its overall success? [Select only 1]

- Critical
- Very important
- Moderately important
- Quite important
- Not at all important
- [Don't know]

- E N D -