

**The
VERITAS
Disaster
Recovery
Research
2004**

**Independent Market
Research Report**

Commissioned by



VERITAS™

**September
2004**

1. Summary

How robust is your DR plan?

Fire disaster scenario: [3.23]

- When presented with a scenario where a fire completely destroys the company's main data centre, an alarming 43% of global companies with DR plans in place had no idea how long it would take them to achieve skeletal operations following such an event.
- And this ignorance is especially common in Asia-Pacific (56%) and US (55%) companies, compared to in EMEA ones (38%).
- Some did volunteer times to recovery, and only 3% think they could carry on with business as usual if a fire were to completely obliterate their main data centre.
- Furthermore, only 28% of companies could achieve skeletal operations within less than 12 hours of such a fire disaster – and more EMEA companies (31%) lay claim to this, compared to US companies (17%).
- In fact, the average time it would take is 3.23 days, and this ranges from immediately to 1 month.
- In terms of the next stage of recovery, only 19% would be able to get mostly back up and running within less than 12 hours of such a major disaster - but, once again, 45% of companies admit they do not know how long it would take them to get mostly back up and running in such a situation.
- In terms of getting completely back to normal, only 12% would be able to get back to 100% normal operations within less than 12 hours of a major fire disaster – but 40% admit they do not know how long this would take.

Business continuity or just technology recovery? [3.3]

- Indeed, some light is shed on the above findings by the fact that only 38% of companies have a DR plan that is integrated with the BC plan – and this is especially common in EMEA companies (42%), compared to Asia-Pacific ones (27%).
- Another 15% of companies only have a DR plan and do not even have a BC plan – especially in Asia-Pacific companies (33%), compared to US (6%) and EMEA (11%) companies.
- And 40% have a DR plan and a BC plan, but they exist as separate plans – especially in US companies (50%), compared to those in the EMEA (40%) and Asia-Pacific (36%) regions.
- Alarming, 7% of these IT respondents who are in charge of their company's DR plan do not even know how the DR plan relates to the BC plan, or if one exists – especially US (9%) and EMEA (8%) companies, compared to Asia-Pacific ones (3%).

Taking steps –DR technology and processes in place: [3.25]

- Yet companies do have a plethora of technology types and processes in place for their DR plans – 96% have at least 1 solution to help them get back up and running as fast as possible following any sort of disaster.
- 87% have a basic backup system in place, but the next most common solution is a fireproof backup storage facility, but only 54% of global companies have such a piece of basic equipment to protect their valuable backed up data.
- 44% have restoration software, 39% have verification software, only 9% use replication and just 5% use clustering technologies.
- 11% have vendor contracts for the replacement of hardware and / or software in the event of a disaster, and another 11% use an outsourced DR company that provides an alternative site, while 11% use an outsourced DR company that will restore the IT systems within a given time frame – such 3rd party solutions are especially common in EMEA and US companies, compared to Asia-Pacific ones.

How effective are DR plans at aiding business continuity: [3.24]

- But even with these various technology and processes in place, 92% of global companies think there would be serious consequences if they had to implement their DR plans in full.
- The Top 5 potential consequences of a disaster striking with their existing DR plans in place are thought to be:
 1. Decreased employee productivity (62%)
 2. Data loss (43%)
 3. Reduction in profits (40%)
 4. Damage to customer relationships (38%)
 5. Reduction in revenue (27%)
- 18% go as far as saying the company's survival would be at risk if a potential disaster were to strike and with the subsequent implementation of the DR plan – especially Asia-Pacific (29%) and US (27%) companies, compared to EMEA ones (14%).

Room for basic improvements: [3.9]

- Many DR plans may well be flawed simply because of where they are stored - 67% of companies keep their DR plan in the main data centre - in fact, 53% ONLY keep the DR plan in the company's main data centre.
- Just 26% keep the DR plan at another company building away from the main data centre – but most are just 10 km away – but this practice is more common in EMEA companies (28%), compared to Asia-Pacific ones (16%).
- 18% keep the DR plan located off-site at a 3rd party's secure location – but again, most are just 35 km away from the main data centre.
- Indeed, 81% of companies keep their DR plan in just 1 of these locations.

- But there has been modest improvement since 2003, with more companies questioned in 2004 (26%) saying that the DR plan is located at another company building away from the main data centre, compared to 2003 (20%).

Testing the plan: [3.4 & 3.5]

- While 91% of the sample test their DR plans, the largest group (34%) only carry out such testing annually - only 17% test as frequently as monthly.
- This infrequent testing may be explained by the fact that 81% of global companies think there are barriers to testing their DR plans.
- The Top 3 barriers are:
 1. Resources, in terms of people's time (49%)
 2. Resources, in terms of budget (32%)
 3. Disruption to employees (29%)
- 19% think that disruption to customers is a barrier to testing their DR plan, and 13% say disruption to sales and the revenue stream is a barrier.
- 13% say other IT projects take a higher priority than testing the DR plan.
- But only 7% say DR testing is not seen as a priority by top management.
- Overall, Asia-Pacific companies say there are more barriers to testing their DR plan, compared to US and EMEA companies – yet these companies still manage to test more frequently than US and EMEA companies.

Real disasters: [3.21]

- Overall, 51% of companies have actually had to execute for real their DR plan, either in full or in part.
- In contrast, 46% have never had to execute their DR plan – especially EMEA companies (50%), compared to Asia-Pacific (36%) and US (33%) companies.
- The most common circumstance for DR plan execution has been computer system failure, such as hardware and software failure (37%).
- This is followed by 26% that have executed their plans due to external computer threats, such as viruses and hackers – and this seems especially prevalent in Asia-Pacific (47%) and US (35%) companies, compared to EMEA ones (20%).
- Indeed, 14% of global companies have executed their DR plan due to natural disasters, such as fire and floods - but almost as many (13%) have implemented the plans due to internal computer threats, such as accidental and malicious employee behaviour.
- And a significant 10% have executed their plans due to man-made disasters, such as war and terrorism - especially Asia-Pacific (21%) and US (15%) companies, compared to those in EMEA (7%).
- Compared to last year, the level of DR plan execution has risen, with more companies questioned in 2003 (65%) saying they had never had to execute their DR plan for real, compared to companies questioned this year (46%).

- Increases during the last year have been for the following types of disaster: natural disasters, such as fire or floods (was 33%, now 51%); man-made threats, such as war and terrorism (was 2%, now 10%); external computer threats, such as viruses and hackers (was 12%, now 26%); internal computer threats, such as accidental and malicious employee behaviour (was 6%, now 13%).

Change-control issues:

The IT system: a dynamic environment? [3.27 & 3.29]

- Overall, 94% of companies apply patches – and 59% apply them at least monthly or more frequently than this – including 17% that apply them daily, 25% that apply them weekly and 21% that apply them monthly.
- Overall, US and EMEA companies apply patches more frequently than Asia-Pacific companies.
- Similarly, 98% of companies make hardware and / or software changes to their systems - 31% make changes at least monthly or more frequently than this - 7% make them daily, 9% make them weekly and 15% make them monthly.

Does change trigger review? [3.7 & 3.8]

- With such dynamic IT environments, one might expect the DR plan to be updated very frequently – indeed, 93% of companies review their DR plan and strategy at some stage or another.
- But the largest proportion (34%) review the DR plan and strategy on an annual basis, another 11% review the plan less frequently than annually, and 4% never review it.
- Only 14% review their DR strategy and plan on a monthly basis – whereas a much greater number of companies apply patches (59%) and make hardware and software changes (31%) at this frequency or even more frequently than this.
- In addition, 17% only test their DR plan as frequently as monthly.
- Yet 35% say they have been prompted by changes in technology to review their DR strategy in the past, but only 5% have been prompted by an increase in patches – however, the latter is especially the case in the US (18%), compared to Asia-Pacific (2%) and EMEA (4%) regions.
- But reviewing of the DR plan is generally becoming more frequent, with more companies questioned in 2004 (14%) saying they review their DR plan monthly, compared to companies that said this in 2002 (2%) and 2003 (7%).
- And, more companies questioned in 2004 (35%) say changes in technology have triggered them to review their DR strategy, compared to companies questioned in 2003 (15%).

Significance of the change-control issue DR? [various questions]

- But change control seems to be an increasingly significant issue:
 - 40% of companies say that changes in technology prompted them to first create a DR plan – especially in the US (49%) and Asia-Pacific (51%), compared to EMEA (36%).
 - 8% have been driven to create a DR plan by an increase in patches – especially in the US (22%), compared to EMEA (7%) and Asia-Pacific (5%) regions.
 - 49% say they would feel exposed to change-control issues, such as patches, if they did not have their plans in place - especially EMEA companies (52%), compared to Asia-Pacific ones (40%).
 - 7% have actually had to implemented their plans due to change-control issues, such as patches – especially in Asia-Pacific (10%) and US (22%) companies, compared to EMEA ones (5%).
- Despite this, 66% of companies that feel exposed to change-control issues, such as patches, have not calculated the potential cost for this threat.

The Board - a false sense of security?

Who really makes the decisions on DR? [3.12]

- When it comes to defining the DR strategy, decision making most commonly rests with the departmental IT manager (52%).
- Only 21% give responsibility to the Board of Directors in the DR strategy decision-making process, and even fewer single out the CEO (8%), other non-IT senior managers (3%) and any non-IT managers below this level (2%).
- But the amount of involvement by the Board has increased since 2003 (was 12% in 2002, 11% in 2003, and now 21%) – and the Board is also more involved in Asia-Pacific (25%) and EMEA (21%) companies, compared to those in the US (11%).
- Also, the role of chief security officer seems to have increased from 2% in 2002, to 4% in 2003, to 9% in 2004.
- But still, a significant 71% of companies only involve IT staff in the decision-making process for the DR strategy of their company.

Signing off the DR plan: [3.13]

- Despite this apparent hands-off approach by the Board and CEO, 75% of companies say the Board has already signed off their DR plan.
- Only 8% say the Board still has yet to sign off their DR plan – but this is especially the case in Asia-Pacific (15%) and US (11%) companies, compared to EMEA ones (5%).
- But, alarmingly, 17% of these IT managers in charge of their DR plans are not sure what the Board's approach is to signing off the company's DR plan.

- Indeed, given the rise of importance of change-control issues, it is worrying that 35% say the DR plan was only signed off by the Board once when the plan was first created – and this is especially the case in Asia-Pacific (37%) and EMEA (36%) companies, compared to US ones (22%).
- And only 11% of global companies say the Board signs the DR plan off every time it is reviewed and changes are made – and this is carried out more in EMEA companies (14%), compared to Asia-Pacific and US ones (both 4%).

Future investment in DR: [3.14 & 3.15]

- While 39% of companies' Boards think there is a need for further investment in the area of disaster recovery (especially in EMEA and Asia-Pacific regions), the same proportion (39%) think the opposite (especially in the US).
- In addition, 22% of IT managers with responsibility for the DR plan are not even sure if the Board thinks there is any need for further investment – especially in EMEA companies (24%), compared to Asia-Pacific ones (15%).
- Among the companies that do think there is a need for further investment in DR, 33% say that, in hard economic times, investment would be reduced, but it would still carry on.
- 16% say all ongoing investment would be frozen and all activity would be put on hold in difficult times - especially Asia-Pacific (22%) and EMEA (15%) companies, compared to US ones (4%).
- Only 22% say all ongoing investment would be maintained and safeguarded.
- But even fewer (6%) say investment might be increased in hard economic times, if deemed necessary – and this is especially the case for US companies (17%), compared to Asia-Pacific and EMEA ones (both 5%)
- But 24% of IT managers were not sure what would happen to the IT investment in DR if hard economic times were to strike.

Knowing what's covered: [3.10, 3.16 & 3.12]

- Most DR plans cover database servers, applications, email, remote offices and web servers, where they exist within a company.
- But fewer include the desktop environment, laptops, mobile technology and home workers' PCs.
- Only 22% of companies cover mobile technologies and only 36% cover the laptop environment.
- Overall, US companies have more of these technologies covered by their DR plans, compared to Asia-Pacific companies – specifically email, web servers, the desktop environment, the laptop environment, mobile technology such as handheld devices, remote offices and home workers' PCs.
- Compared to 2003, more companies are covering email (was 39%, now 78%); the desktop environment (was 20%, now 53%); and the laptop environment (was 14%, now 36%).

- In fact, IT managers seem very confident that the Board is well informed, with 74% saying the Board is fully aware of what is covered in the DR plan – an opinion that is especially common among Asia-Pacific companies (81%), compared to EMEA (72%) and US (65%) ones.
- Only 11% say the Board is not well informed, and many of these do not think the Board even need to know – and this applies to more US companies (19%), compared to Asia-Pacific (7%) and EMEA (11%) ones.
- Another 15% say they are not sure whether the Board is fully aware of what is covered and what is not.

Is your desktop a priorities? [3.26]

- While there is a wide variety of opinion on which applications are a top priority to get back up and running following a disaster, three emerge as front runners: telecoms (53%), finance and accounting (53%) and security systems (50%).
- Indeed, these are followed by email, and in fact, more companies put a high priority on email (34%) for restoration than they do on basic office applications (29%).
- 29% put a top priority on sales and marketing, whereas only 19% put the HR systems as a top priority.
- Overall, US companies place more of these applications as a top priority, compared to Asia-Pacific companies.

Suppliers – an Achilles’ heel? [3.30]

- Even if companies take care of the data within their own company, most neglect any company data that is held by various suppliers.
- Indeed, 28% of companies do not ask to see the DR and BC plans of any of their third party suppliers, and they just assume they exist and are adequate – and EMEA companies seem to be the most trusting with more of them (33%) making this assumption, compared to Asia-Pacific (18%) and US (16%) companies.
- Another 12% are unsure about the degree to which the BC and DR plans of suppliers are given consideration by their company.
- In contrast, 32% say they ask to see the BC and DR plans of the technology suppliers to their company before they start work with them – and this practice is especially common in the US (62%), compared to in the Asia-Pacific (36%) and EMEA (27%) regions.
- But, even fewer (15%) ask to see the DR and BC plans of their DR outsourced partners – but Asia-Pacific (22%) and US (36%) companies seem more formal in this respect, compared to EMEA companies (11%).