



Business continuity

Be resilient, be reliable, be ready for anything!

A Datamonitor white paper prepared for



Publication Date: November 2003

www.datamonitor.com

Datamonitor USA
1 Park Avenue
14th Floor
New York, NY 10016-5802
USA

t: +1 212 686 7400
f: +1 212 686 2626
e: usinfo@datamonitor.com

Datamonitor Europe
Charles House
108-110 Finchley Road
London NW3 5JJ
United Kingdom

t: +44 20 7675 7000
f: +44 20 7675 7500
e: eurinfo@datamonitor.com

Datamonitor Germany
Messe Turm
Box 23
60308 Frankfurt
Deutschland

t: +49 69 9754 4517
f: +49 69 9754 4900
e: deinfo@datamonitor.com

Datamonitor Asia Pacific
Room 2413-18, 24/F
Shui On Centre
6-8 Harbour Road
Hong Kong

t: +852 2520 1177
f: +852 2520 1165
e: hkinfo@datamonitor.com

ABOUT DATAMONITOR

Datamonitor plc is a premium business information company specializing in industry analysis.

We help our clients, 5000 of the world's leading companies, to address complex strategic issues.

Through our proprietary databases and wealth of expertise, we provide clients with unbiased expert analysis and in-depth forecasts for six industry sectors: Automotive, Consumer Markets, Energy, Financial Services, Healthcare, Technology.

Datamonitor maintains its headquarters in London and has regional offices in New York, Frankfurt and Hong Kong.

INTRODUCTION

The business continuity planning and disaster recovery (BCP/DR) market has been thrust into the limelight by recent terrorist atrocities but, in truth, is being driven more by the continuing trend among all organisations to tie IT systems more closely with their business processes. As companies look to new and existing applications and systems to increase efficiency, lower costs and create new business so they open themselves up to new risks. As their operations continue to depend heavily on their IT infrastructure, any system downtime can badly affect the organization's well being.

Datamonitor believes that the resultant need to ensure that downtime is minimised will drive the business continuity and disaster recovery markets forward and that the Western European market will grow from \$2.7bn in 2002 to \$6.8bn in 2005, at a CAGR of 37%. The UK was the largest market in this region in 2002, representing 26% of the market's revenues (\$689m) largely thanks to strong spending by financial services institutions and an increased sense of insecurity with regards to terrorism. France was the second largest market, representing 16% of the market (\$430m), while recession in Germany limited spending to an estimated \$398m (15% of the market).

This paper will enable readers to:

1. Understand what business continuity and disaster recovery entails and what **products and services** the BCP/DR market is comprised of;
2. See what powerful forces are **driving the market forward** and how important the market is in terms of revenues;
3. Determine how **IT security** is also an integral part of any strategy to maximise system uptime;
4. See why the **financial services sector** generated 60% of European BCP/DR revenues in 2002 and why regulations such as Basel II continue to drive the market forward.

BUSINESS CONTINUITY DEFINED

What do we mean by business continuity and why has it become so important to many businesses?

The concept of business continuity and resilience is relatively new and has been spurred on by the increasing use of IT by enterprises and the resulting vulnerabilities that it exposes enterprises to. While the financial services space has been a strong consumer of business continuity planning and disaster recovery (BCP/DR) products and services, new industry sectors are emerging and the product mix is changing. The focus is shifting away from hardware-based resilience and simple backup & restore solutions to IT architectures that are resilient to data corruption or loss and are less likely to fail as a whole. A great deal of the investment is linked to the increasing need to control operational risk, particularly among financial institutions.

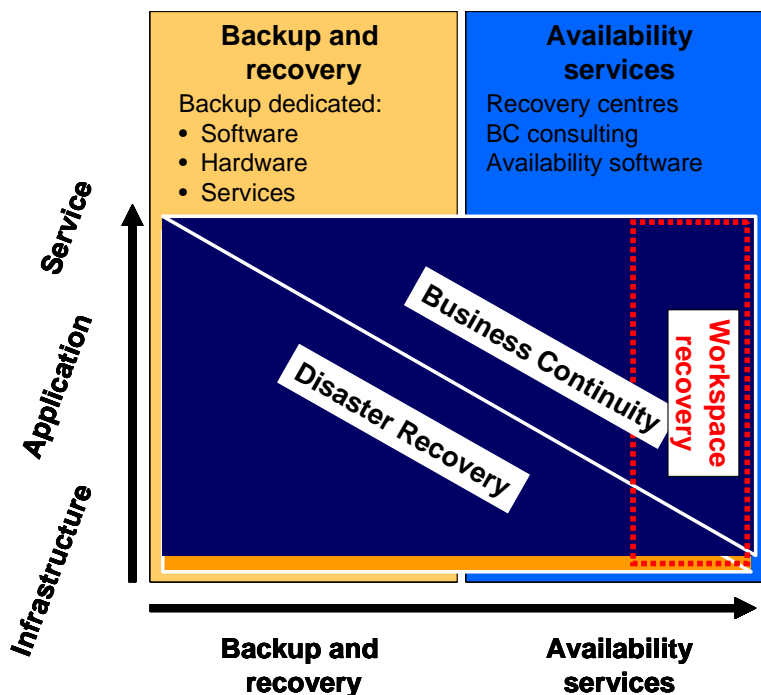


Figure 1: Business continuity defined

Source: Datamonitor

DATAMONITOR

Because business continuity as a product is largely intangible, the critical starting point in any examination of the business continuity market is to gain an understanding of the market segmentation. Business continuity, as a concept, is the collection of corporate values and frameworks supported by an infrastructure of resilient hardware and software, combined with contingency plans that support a set of given business processes. Therefore, the business continuity planning and disaster recovery market is the supply of complementary services and products that help businesses recover from a disaster or disruption and that also support the quest to minimise the occurrence of disruptions in the first place

Business continuity – a shift in emphasis from back-up and restore to constant uptime

The overall BCP/DR market cannot be split between business continuity planning and disaster recovery, due to the significant functional overlaps between the two. For this reason Datamonitor has segmented the market by function as follows:

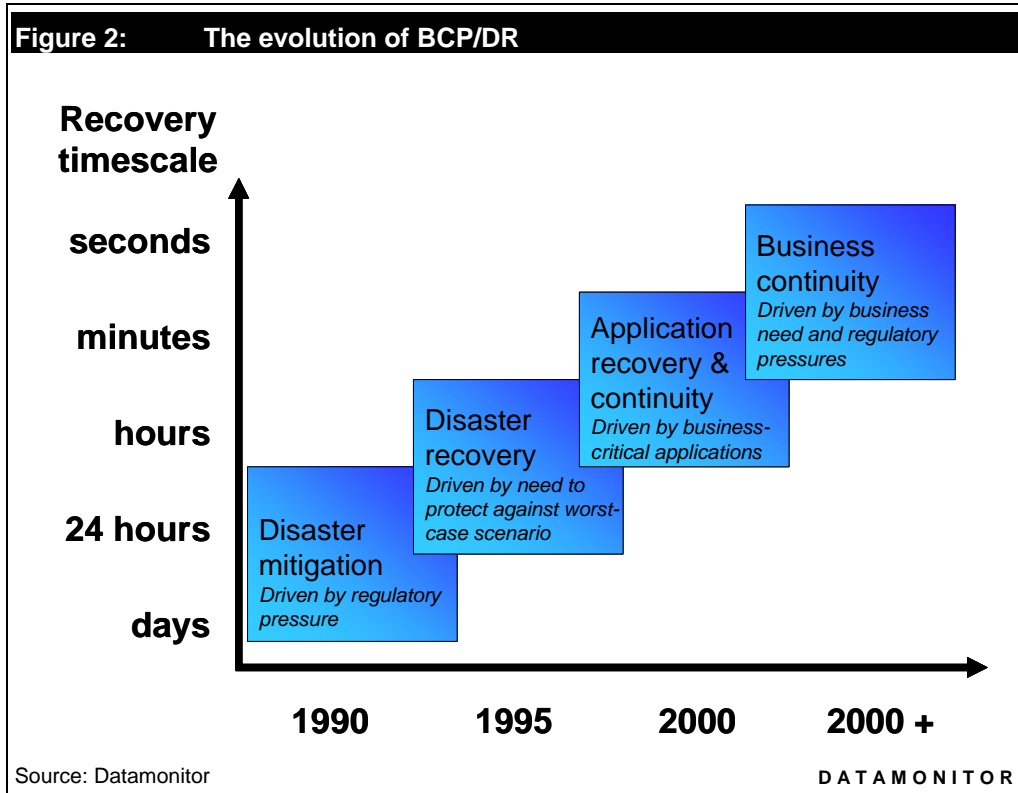
- backup & recovery – covering the dedicated software and hardware for creating backups for and recovering data, as well as dedicated third-party backup & restore services;
- availability services & products – the supplying of products and services intended to ensure increased resilience and the supply of services, other than backup and restore, to restore business operations in a disaster.

Backup & recovery

The backup & recovery market is the supply of dedicated backup and recovery devices, software and related services. This includes recovery centres, where the customer has a remote copy offsite that can be restored on the customer's premises. If the data, application or process that has been backed up to a remote site is subsequently operated offsite, the resulting spend is counted as availability services. Backup & recovery would therefore not include general hardware used for backup or plain storage, like tape libraries or RAID arrays, infrastructure spend, general network management software, redundant hardware and fibre channel switches (unless these perform server-less backup).

The backup & recovery market is larger than the availability services & products market, but is also more mature, and hence more commoditised, heading towards flat

revenues by 2005. This is especially the case in more developed markets like the UK and Switzerland, resulting from the strong presence there of financial markets.



Availability services & products

The availability services & products market is the supply of services enabling companies to maintain business operations despite disruptions:

- **Recovery centres.** Off-site locations where data, applications or processes are run or maintained by or at a third party site in case the primary in-house site is unavailable;
- **Software.** Organisations can also deploy software that has the sole purpose of maintaining or managing the integrity and flow of data in the event of a disruption;
- **Consulting services.** These are designed to help organisations formulate their business continuity policies and plans. Pure outsourcing is not counted at all in the BCP/DR market.

The availability services market in Europe is relatively speaking quite young, with the main exception of the UK where the high concentration of financial services companies in the City of London and the threat of IRA terrorism created an earlier market need. As a result, the market will grow strongly in the financial services sector at almost treble the growth rate of the backup and recovery market.

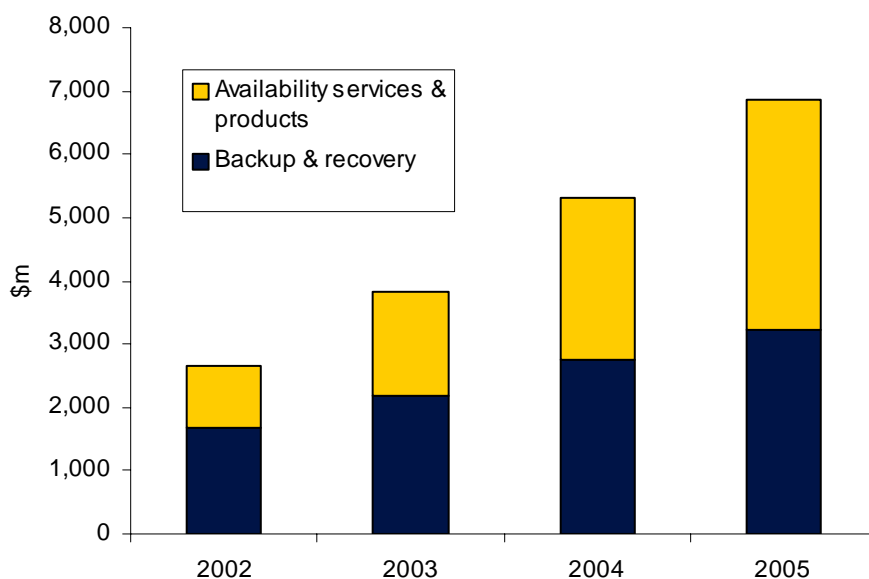


Figure 3: Estimated business continuity & disaster recovery expenditure in Europe 2002-2005 (\$m)
 Source: Datamonitor DATAMONITOR

	2002	2003	2004	2005	CAGR
Backup & recovery	1,663	2,183	2,757	3,240	25%
Availability services & products	1,008	1,653	2,552	3,608	53%
Total	2,672	3,836	5,309	6,848	37%

Source: Datamonitor DATAMONITOR

What is driving the strong growth in business continuity spending?

The main factors that are driving business continuity can be summed up as follows:

- **Globalisation.** With many large enterprises increasingly establishing a more global presence and IT systems simultaneously being integrated more closely with business processes, globalisation is raising the stakes in the event of a system shutdown. With regional centres operating in different time zones, the network needs to be fully available on a 24/7 basis;
- **The move towards 24/7 business.** With the Internet, customers have become accustomed to accessing information and services all day, everyday. As a result maintenance and backup windows are diminishing;
- **Operational risk and Basel II.** Within the financial services sector, the new accord for capital adequacy for banks is groundbreaking in that it specifies risk not only in terms of capital risk but also in terms of operational risk. The requirements to map and contain operational risk mean that Basel II has a direct impact on the business continuity market. Other industry sectors are closely monitoring the situation to determine how Basel II improves business continuity in the financial services sector with a view to creating similar regulations themselves;
- **Terrorism.** While terrorism is not the main driver for BCP/DR (and certainly not a new one in the UK), it very publicly and clearly underlines the impact of uncontrollable events on an enterprise's business processes. The unfortunate events of 9/11 have once again brought the problems of terrorism to the forefront of people's thinking and raised the awareness at board level for the need to understand and invest in resilience.
- **Insurance.** Most companies understand that if they invest in burglar alarms and security guards, the more rebate they get on their premiums. As business processes become more aligned with technology, companies are increasingly looking to mitigate their "cyber-risk" with dedicated security policies. A comprehensive business continuity strategy will help firms convince their insurers that they are taking the appropriate steps and can help to reduce the overall premium that they are charged.

Despite the recent return of terrorism as a threat high in businesses' awareness, the underlying drivers for BCP/DR spend, increased globalisation, 24/7 business and increased process automation have had and will continue to have a more powerful effect on the BCP/DR industry. This is largely due to the fact that the positive benefits of good BCP, i.e. more efficient and continuous business, remain a stronger driver to invest in BCP/DR than the threat of terrorism, although the latter has been effective in bringing the topic into the limelight.

BUSINESS CONTINUITY IN AN IP WORLD

One important trend in recent years has been for companies to look at new and innovative ways of reducing the cost of communications while adding feature-rich applications that improve the employee's user experience. Network convergence, whereby voice, video and data traffic are run as IP across a single data network is an important means of achieving this goal. Datamonitor's view is that organisations choosing such solutions can not only streamline internal business processes and improve collaboration but can also help the company monitor, manage and optimize activities across a number of different networks, involving customers, suppliers and partners.

Switching to IP, however, carries with it important business continuity connotations, both of a positive and negative nature. Firstly, one of the main inhibitors to network convergence in the past has been the worry over the reliability of data networks in general. Most circuit switched networks, for example, are 99.999% reliable – something that few data networks can achieve. Furthermore, when they go down, only voice connectivity is lost. In contrast, converged networks are still seen as less reliable. At the same time, converged networks by definition carry both voice, video and data traffic. When such networks fail, all of that network's users instantly lose the ability to communicate with the outside world, including via voice (except through cellular devices). Given the gravity of such a failure, business continuity measures such as back-up Internet connections and equipment clustering in the event of core network failure are critical to ensuring the resilience and high levels of uptime that today's enterprises demand.

Running all traffic over an IP network can, however, has important business continuity benefits as was highlighted by the September 11th disaster. Firms such as Merrill Lynch who had converged their voice and data networks could simply transfer affected workers to new sites or ask them to remain at home and they would instantly have data and telephony network capabilities including instant call transfer and

unified messaging. This capability greatly reduced the impact of the disaster on those organisations affected and meant that the firms could get their employees back up and running in a much shorter timeframe than would have been traditionally possible.

THE IMPORTANCE OF IT SECURITY IN BUSINESS CONTINUITY

While much of business continuity focuses on organisations' attempts to deal with disasters once they occur and minimise the effect they have on IT operations, IT security solutions are designed to proactively protect IT assets from some very specific threats. The following diagram examines some of the key threats that businesses may face: both of an accidental / unintentional nature and those which are deliberately designed to damage or hamper the IT system. IT security solutions are specifically implemented to protect organisations against intentional, electronic threats such as viruses, web defacement and denial of service attacks.

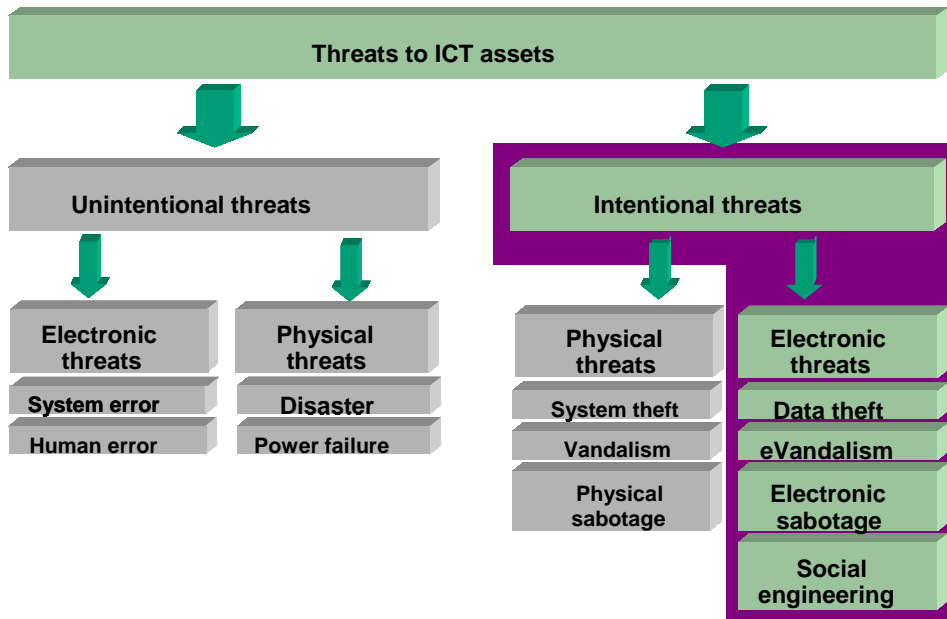


Figure 4: The key threats to IT assets

Source: Datamonitor DATAMONITOR

The IT security precautions that organisations can take fall into three principal categories:

Business continuity and disaster recovery white paper - BT

© Datamonitor (Published November 2003)

This report is a licensed product and is not to be photocopied

- **Products.** Most organisations have invested in IT security products as a means of protecting themselves from potential security threats such as viruses and hackers. Anti-virus and firewalls are the two most common forms of security products deployed, although investment has increased in complementary technologies such as vulnerability assessment and intrusion protection solutions as companies look for more serious protection. The IT security products that an IT department deploys are known collectively as the security architecture and while it is possible to buy several components from a single vendor, it is more common to purchase the best product of its type to create a 'best-of-breed' portfolio.
- **Services.** Products by themselves are not enough to protect the IT system: they must be correctly installed, configured, maintained and managed. Given the constantly evolving nature of both threats and the technologies deployed to mitigate the risks they represent, organisations often turn to third-parties to provide them with such services. The most common services offered by these professional services firms include security consulting, integration, maintenance, education & training and managed security services.
- **Internal processes.** While security products and services can do a great deal to protect the IT assets from attack, the behavior of IT users can still be modified to reduce the risk of virus propagation, the unauthorized use of IT assets and the threat from social engineering. The embodiment of this process is the IT security policy, which most European organisations have deployed as the basis of their security strategies. Internal processes also include the services carried out by the organization's own IT staff, escalations procedures and internal risk assessment audits.

One important part of the internal process is the creation and implementation of an IT security policy. This policy often takes the form of a document distributed via email or published on the organization's intranet and advises the organization's employees on what is considered to be appropriate system and Internet behaviour. Such a policy is particularly important given that the users themselves are often considered to be the weakest link in the security chain. A well-maintained policy document can warn users against opening suspicious emails or leaving PCs "unlocked" when the user is away.

While many vendors and professional services firms tend to differentiate their BCP/DR solutions from the rest of the security market. IT security breaches represent a significant threat to the continuous operation of the IT system. As such, security should be considered an integral part of any strategy designed to ensure maximum uptime.

THE BCP/DR MARKET IN EUROPE

The overall Western European business continuity and disaster recovery market is set to grow from a base of \$2.67bn in 2002 to reach \$6.85bn in 2005, growing at a CAGR of 37%. The UK is the largest market, accounting for just over a quarter of BCP/DR spend in 2002. The size of the UK market is accounted for by several factors, mainly the sheer size and concentration of the financial markets in London. The IRA campaign against economic targets around the UK, particularly in London, has contributed to making organisations that form part of the country's critical infrastructure (financial services institutions, utilities and government agencies) aware early on of the risks of disaster and the need to take preventative measures.

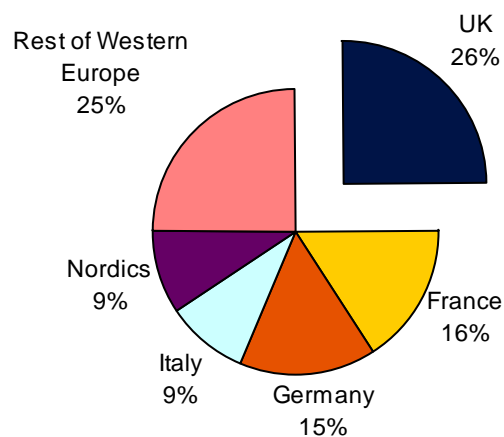


Figure 5: The Western European BCP/DR market by country

Source: Datamonitor

DATAMONITOR

BCP/DR spend is particularly high in financial markets in the UK. At almost double the size of other country markets in Europe, the UK has the most sophisticated BCP/DR customer base in Europe and arguably the world. Despite the fact that the level of existing BCP/DR cover in the UK is already high, the market will continue to grow at steadily. However, the spending in the UK will be focused more on retail banking and

insurance, in line with overall European trends, which will grow at a rate of 27% and 23% respectively between 2002 and 2005.

The BCP/DR market in Germany in 2002 was disproportionately small compared with the size of the overall market. The current poor performance of German financial services institutions has dampened the pace at which progress has been achieved, and problems with work councils and outsourcing have resulted in German institutions spending more in-house than average in other European countries. Germany is, however, one of the largest consumers of ICT solutions and German firms have been very forward thinking in their application of technology to enhancing business processes. Datamonitor therefore believes that businesses in this market will increasingly look to business continuity going forward as the economy improves and as Germany customers develop a greater understanding of the need to protect previous IT investment with BCP/DR. The strong growth in BCP/DR investment in Italy as a whole has been strongly influenced by the rapid consolidation of the retail banking industry, and more advancement of IT investment across all areas of banking and insurance is driving overall data volumes up and increasing management issues in the process. As a result, this increased complexity in the system has been driving and will continue to drive up the cost of securing the systems in place as the market continues to mature and catch up with other European markets.

BUSINESS CONTINUITY BY VERTICAL MARKET

While all organizations seek to minimise disruption to their operations, for some the loss of their systems could be more than just an irritation – it could be a crisis with far-reaching consequences. Governments have long looked at certain industries and have sought to ensure that these sectors take business continuity issues seriously as they form what can best be described as a nation's critical infrastructure. There are three key groups that fall into this category.

- **Government services.** It is the government's responsibility to provide a large number of services to its population that if disrupted could have severe consequences for the economy or even lead to loss of life. Examples of services that cannot afford any disruption include the police, fire and ambulance services as well as defence, the justice system and social security.
- **Utilities.** Another sector of the economy that cannot afford any disruption to its services is utilities offering water, gas, electricity and communication services to a nation's population. Governments have been aware for a long time of the potential of these organizations as terrorist targets and after September the 11th

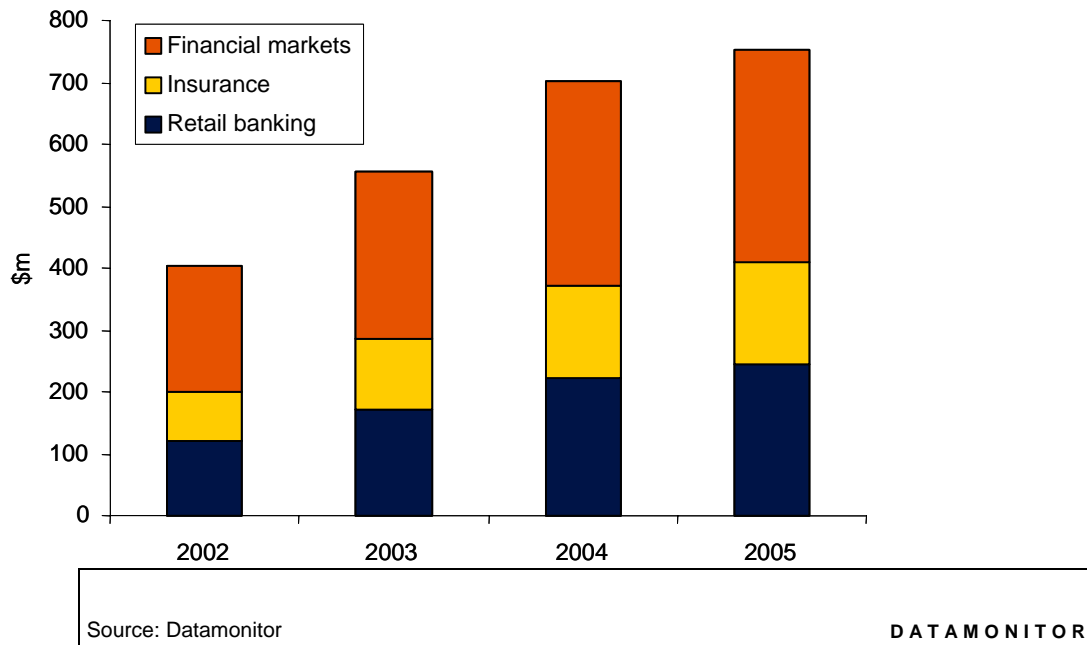
many western governments have been keen to push this message home. Recent dramatic power cuts in the US, UK, Sweden and Italy reinforced the need to ensure that utility firms take continuity more seriously.

- **Financial services.** A thorough risk assessment programme is a prerequisite for any business continuity strategy and financial services firms have always been more aware of risk when conducting business and operational risk in particular. Regulatory forces have also been aware of the importance of the interdependence of different financial institutions and the systemic risk this creates and have been keen to force financial services firms to adopt means of reducing operational risk. The US government, for example, expressed a great deal of concern over the news that the SQL Slammer worm paralyzed Bank of America's ATM network, making it unable to process transactions.

Business Continuity in financial services

The financial services sector has always been at the leading edge in the use of business-orientated technology. Therefore, it is logical that financial services companies have the most developed approach to BCP/DR of any vertical market. Investment in backup and restore solutions and availability products and services is driven by the high value of the systems in question, and enforced by financial regulators. These drivers have created a powerful demand for BCP/DR solutions among financial services institutions (FSIs) and has created a market worth approximately 60% of the total Western European market in 2002.

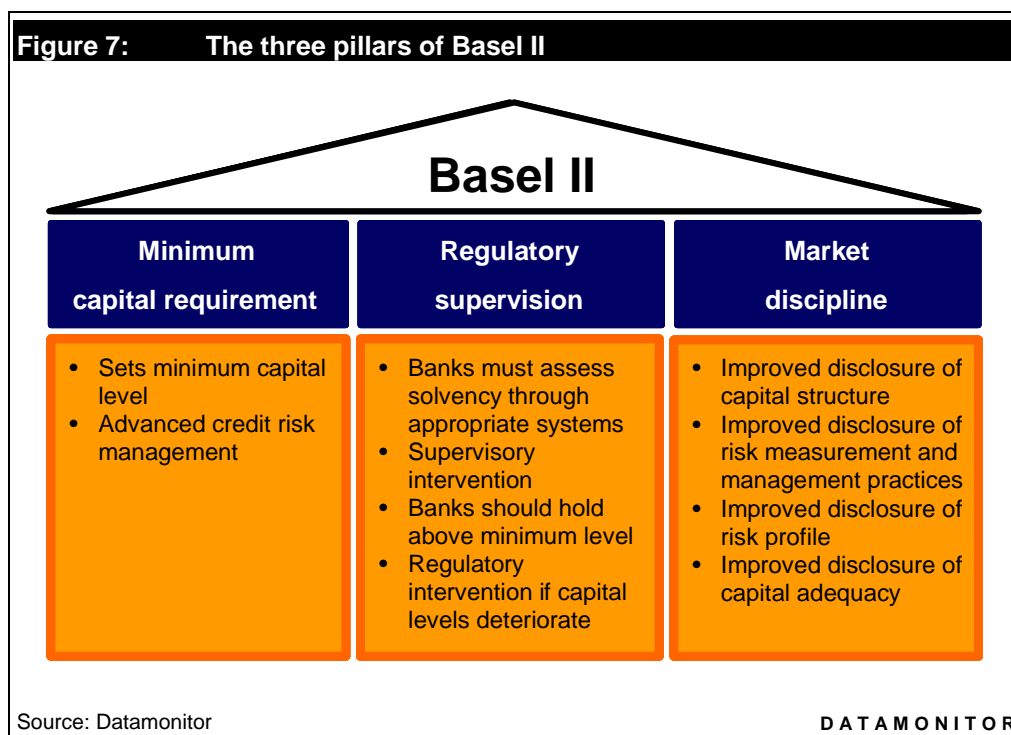
Figure 6: The UK BCP/DR in FS market 2002-2005 (\$m)



One critical development in recent times has been moves by central bodies from certain industry sectors to help ensure that organisations are better protected from the numerous risks that they face to their operations. This may be on a national level (such as the Financial Services Authority (FSA) in the UK) or on a global level such as the second report from the Basel Committee for Banking Supervision (BCBS) on risk management (otherwise known as Basel II).

From 2007, the Basel II framework will determine what proportion of their assets banks must set aside as a reserve to guard against credit, market and operational risk. The realisation that risks, other than credit and market risk, could be substantial prompted the committee to assess operational risk as a discrete category for consideration under the new accord. As IT-related business continuity is inexorably linked to operational risk, and the mitigation of that risk, there is a direct connection between business continuity and Basel II. The Basel II accord is build on three pillars:

- minimum capital requirement;
- regulatory supervision;
- market discipline.



The new framework that Basel II sets up, from a business continuity point of view, means that financial institutions must be able to prove to the regulatory supervisors that they have sufficiently comprehensive and secure systems in place to assess operational risk. While there is no specific mention of business continuity in the Basel II accord, it is widely understood that IT investment will have to occur in order to ensure that improved reporting tools required for compliance are in place. Furthermore, IT investment will be required in order for financial institutions to be able to give tangible quantification of actions taken to lessen operational risk that IT poses.

While business continuity solution providers in Europe look forward to a dramatic increase in spending by FSIs, in the United States the impact of the regulation will be much less dramatic. The Federal Deposit Insurance Corporation, the US FSI regulatory body, has decided not to impose the accord on all but the largest organizations that it oversees. This will dramatically reduce the level of spending on BCP/DR solutions in the US with few companies looking to increase investment in an area that they are not forced to by the threat of an increased minimum capital reserves which would effectively reduce the amount of money they could lend and therefore generate.

While the FDIC is happy to suggest the principles of the accord to all of its members and does not deny that it would like all institutions to take operational risk more

seriously, it disagrees with the way the Basel II accord seeks to achieve this. Therefore, while there will almost certainly be some impact on BCP/DR spending in the US it will not be to the same degree as in Europe.

ROI FOR BUSINESS CONTINUITY

As with all major technology implementations prospective customers for BCP/DR solutions are demanding to see whether or not they can achieve a return on their investment before deciding whether to go ahead or not. Many companies have previously invested heavily in technologies that have failed to live up to their revenue-generation potential and are keen to reduce overall costs rather than invest in new solutions with no proven effectiveness.

As with IT security solutions it is very difficult to come up with definitive ROI calculations because most of the benefits derived from such BCP/DR systems are only achieved should a disaster occur. If the business continuity or disaster recovery solution works as planned then the costs of the disaster are reduced. Sadly, few companies outside of the core verticals such as the government, financial services, utilities and pharmaceuticals are prepared to invest heavily in precautions against events that may never happen.

In doing so, the impact of any incident will be much greater than for those who take BCP/DR seriously but this is a risk that many companies are prepared to take rather than potentially spend money on solutions that they'll never need. When companies are, however, looking to understand the ROI argument for BCP/DR they should compare the overall cost of any solution to estimates of the potential loss they could incur from temporary or long-term downtime. While some costs are easier to spot and calculate, others are less obvious. The loss of a system for a few hours is likely to impact operations in the short term but is also likely to cause consternation among shareholders about the stability of long-term operations. The following diagram shows some of the tangible and intangible, direct and indirect costs that could be avoided with an effective BCP/DR architecture.

Figure 8: ROI calculation criteria for BCP/DR

	Tangible costs	Intangible costs
Direct costs	Loss of user productivity Loss of potential revenues Loss of data	Loss of customer / partner confidence Employee dissatisfaction
Indirect costs	Supply chain inefficiencies Regulatory penalties Higher insurance premiums	Loss of shareholder Loss of board confidence

Source: Datamonitor DATAMONITOR

DATAMONITOR CONCLUSIONS

Business continuity has evolved from simple back-up and restore to a means of ensuring continuous uptime

The previous response to any loss of availability was to grit your teeth and bare it – and if data was lost, to simply restore it from backed-up archives. In the modern, global economy, however, the need for constant uptime has meant that this situation is now untenable and every effort must be made to reduce downtime to seconds not hours and, if possible, to eliminate it all together.

Fears over terrorism are important drivers but other factors are more important

The effects on businesses caught up in the September 11th tragedy served as a sober reminder of the need to ensure that should facilities be damaged or destroyed, the IT system must continue to operate or the business may fold. Despite being the most high profile reason, the move towards global business practice and the need for 24/7 data and application availability will be the more powerful drivers going forward.

IT security can be a proactive means of preventing system downtime and is highly complementary to BCP/DR

Bombs, floods and fires are not the only means of disrupting IT operations – viruses, denial of service attacks and hacking incidents can be just as effective. With the strong awareness of the need to increase security, many business continuity solution providers will be able to use security as a hook into the wider BCP/DR environment. Because availability is one of the core needs that customers use security solutions to fill (the others typically being data confidentiality and data integrity), the fit between the two worlds is natural.

The UK is the most mature market in understanding the need for business continuity

The UK is the most mature market in terms of accepting the need for BCP/DR and generates over a quarter of all Western European revenues. Two of the biggest factors in this have been the previous terrorist violence waged by the IRA and the importance of the financial markets sector in London. The support of the UK for the US in its war on terror has meant that British businesses may also be targeted. This is something that organisations in the finance world, telecoms, water, gas and electricity and the government will take more seriously as they form the backbone of the nation's critical infrastructure.

The financial services sector is the most important single vertical in terms of BCP/DR market revenues

Because of the high reliance of the FS sector on its IT systems and because of a fundamental understanding of the nature of risk (and the need to mitigate it) financial services institutions (FSIs) represented around 60% of all BCP/DR revenues in Western Europe. Going forward, the need to ensure constant uptime will become increasingly important as regulations such as Basel II force FSIs to take more responsibility for any downtime in their systems – to the extent that they may be penalized financially by being forced to hold more financial assets in reserve. This will reduce their potential to earn money – the most powerful driver for any IT investment.