Business Continuity Planning

Data Protection and Disaster Recovery

An IDC White Paper
Sponsored by Hewlett-Packard

Analysts: John McArthur, Robert C. Gray, and Vernon Turner

EXECUTIVE SUMMARY

When information systems are unavailable, today's enterprise is "out of business." Revenue stops flowing, profits erode, customers cannot be served, and staff go idle enterprisewide. As a result, enterprises should take special care to examine their business continuity plans. With respect to information systems, the cornerstone of system resilience is a plan to protect data and the systems that store it and to provide for disaster recovery when regional outages render an entire datacenter unavailable.

Protecting systems is accomplished by eliminating single points of failure in servers, storage systems, and networks. Redundant hardware and networks, along with alternate sources of electrical power and network connections, make the datacenter resilient. IT operating procedures reinforce the datacenter's robustness.

Disaster recovery plans address the possible loss of a datacenter. Plans include alternative facilities and staff and depend on a recent copy of relevant enterprise data. How recent the copy of data should be depends on the cost of downtime for an application and the acceptable size of the gap between the last copy of data and the onset of the outage.

Enterprises need not "go it alone" with respect to business continuity planning. Third-party providers of remote storage and processing facilities can be used to augment enterprise resources. A trusted partner can improve IT system resilience and often at a cost savings, particularly for the midsize enterprise.

Three case studies highlight the different ways in which enterprises implement data protection and disaster recovery plans and also reveal some unexpected benefits and paybacks.

IDC
Analyze the Future

5 Speen Street • Framingham, MA 01701 USA • Phone 508.872.8200 • Fax 508.935.4015 www.idc.com

INTRODUCTION

BCP requires the development and application of procedures and technologies to ensure that critical information systems will remain available or can be brought back into service quickly when disruptions, such as power outages or network failures, occur.

Business continuity planning (BCP) spans all enterprise operations, including IT, and often extends beyond the enterprise to include business and IT operations of trading partners. With respect to IT, BCP requires the development and application of procedures and technologies to ensure that critical information systems will remain available or can be brought back into service quickly when disruptions, such as power outages or network failures, occur. Procedures must be in place to organize staff, ensure their safety, equip them to communicate during a crisis, and prepare them to move to secondary sites and systems when necessary.

Data protection and disaster recovery are key parts of BCP and are the focus of this paper. Data protection is about designing systems and procedures that ensure ongoing access to corporate information. Disaster recovery is the complementary process of ensuring that information systems and applications can be restored quickly when regional or sitewide outages occur. While the enterprise IT department bears primary responsibility for BCP, third-party outsourced service providers often play important roles as well.

Critical Information Systems

IT's business continuity plans have traditionally focused on critical information systems, which include financial accounting, enterprise resource planning (ERP), and other enterprisewide, large-scale business applications. These applications are often hosted in a datacenter and, in the past, ran in a batch mode or as online transaction processing (OLTP) systems during business hours. Between batches and after hours, databases, files, or data sets could be replicated and copies moved to other datacenters either directly across WANs or shipped on removable media, such as magnetic tape. Disaster recovery meant the ability to restore corporate data, perhaps at another location, to resume processing.

Businesses have come to realize that unavailable information systems can have an immediate negative impact on revenue and profit, disrupt customer care, harm the company's reputation, and decrease productivity.

Today's IT business continuity plan faces new challenges. Midsize and large enterprises have become more dependent on information systems for everyday operations. Thus, the number of companies in need of BCP and the number of systems deemed critical both have increased sharply. Businesses have come to realize that unavailable information systems can have an immediate negative impact on revenue and profit, disrupt customer care, harm the company's reputation, and decrease productivity, as the following examples illustrate:

- Failure of ecommerce systems, point-of-sale systems, or epayment systems puts the enterprise out of business for the duration of the outage.

- Interruptions in rapid replenishment inventory management and other modern supply chain technologies make networks of enterprises vulnerable to each other's IT interruptions.
- As customer care is increasingly supported by information systems, the risk of losing a customer due to network downtime is increasingly of concern.
- When applications such as email are unavailable, enterprises are unable to communicate both internally and with their customers and trading partners.

Eliminating Single Points of Failure

Critical systems are resilient when single points of failure are minimized or eliminated. Clearly identified redundancies in all key systems and subsystems along with procedures that make replicas of data available in case they are needed are central to business continuity plans.

Business continuity plans include redundancy within the datacenter to mitigate risks, such as hardware failure or user error. Plans also address the risk that the entire datacenter becomes unavailable and that IT systems must be hosted at another location.

Plans ordinarily include datacenters dispersed geographically and sized such that one or two centers can carry on business operations if a third center becomes unavailable.

For large, nationwide, and global enterprises, plans ordinarily include datacenters dispersed geographically and sized such that one or two centers can carry on business operations if a third center becomes unavailable. Replicas of data are moved among the datacenters on a regular basis. For the most critical systems, one datacenter may provide a hot backup to the primary datacenter with the ability to take over processing within a few seconds. For less critical applications, replicas of data may be stored on removable media with the understanding that systems can be returned to service after a few hours or even days without great harm to business operations.

Augmenting in-house capabilities with outsource providers is an especially appropriate strategy for small enterprise BCP.

For smaller enterprises that may conduct business from a single location, plans may include third-party outsourced service providers that participate in data replication and maintain geographically dispersed facilities on behalf of their clients. Efficiency and budget dictate that midsize enterprise IT organizations are often small. Augmenting in-house capabilities with outsource providers is an especially appropriate strategy for small enterprise BCP.

Redundancy vs. Cost

Best practices in BCP dictate that the degree of resiliency should be provided in proportion to the cost or consequences of downtime, or the value of continued, timely access to information.

Business continuity planners must find the right balance between cost and redundancy. Eliminating single points of failure means purchasing and maintaining redundant systems. Best practices in BCP dictate that the degree of resiliency should be provided in proportion to the cost or consequences of downtime, or the value of continued, timely access to information. When real-time settlement systems in financial services become unavailable, for example, there is an instantaneous and severe impact on the central mission of the

enterprise. Affording duplicate or triplicate investments in IT for financial services companies is sometimes proscribed by regulation and often viewed as a basic cost of doing business.

Other applications may hamper enterprise operations but not as severely. Monthly payroll and time-reporting applications are less critical to the daily operations of most enterprises. For systems that can be out of service for hours or days without a negative impact on the enterprise, routine backup and offsite storage of data and applications may be entirely adequate. The higher expense associated with closely coupled, highly resilient datacenters would be wasted in such a case.

New IT Infrastructure Technologies Address BCP Issues

Improvements in IT infrastructure are helping to make systems more resilient at a lower cost.

As enterprises review their business continuity plans, IT managers will be pleased to see that improvements in IT infrastructure are helping to make systems more resilient at a lower cost. For example, the trend to consolidate storage that was previously distributed and attached directly to servers sets the stage for simpler and better data protection schemes. Rather than backing up server-attached storage from a multitude of departmental email servers, for example, IT storage managers can utilize a storage area network (SAN). Inside the dedicated storage network, large amounts of data, including departmental email databases, can be replicated to protect from device failure, provisioned with respect to capacity as well as speed, and migrated to alternate media and locations for safekeeping.

THREATS AND COUNTERMEASURES FOR BCP

The IT business continuity plan identifies threats to information systems along with corresponding countermeasures. Threats to business continuity include outages that are unplanned and planned. In addition, business volatility makes the continuity planning process particularly difficult. Countermeasures are a mixture of system design, IT operating procedures, and third-party services. Threats and countermeasures will be examined in detail.

Threats

Murphy's Law and its many corollaries summarize the real concern of IT managers: Anything that can go wrong will — and probably at the worst possible moment.

Traditional disaster recovery plans focused on unplanned downtime for good reason. Murphy's Law and its many corollaries summarize the real concern of IT managers: Anything that can go wrong will — and probably at the worst possible moment. As Table 1 shows, a multitude of factors can interrupt IT services.

Unplanned downtime may result from threats directly under the IT department's control (e.g., the threat of a subsystem or component failure). Other threats — for example, the loss of electrical power or network access — lie outside the direct control of the IT organization, although the IT department's business continuity plan must include and address them. Software and operator error can often wreak havoc unexpectedly by corrupting data or failing to store or move data properly.

Table 1: Three Categories of IT Services Outage

Unplanned Downtime	Planned Downtime	Business Volatility
• Loss of electrical power or WAN services • Failure of processing, storage, or network devices • Accidental (or purposeful) corruption of data due to operator behavior; corruption of data due to software fault or virus • Rolling outage caused by failure of a trading partner's IT system • Intermittent outages, especially those occurring during data recovery processes	• Maintenance and upgrades for system and application software • Installation of new or replacement hardware components • Backup and restore procedures for consolidated and distributed storage	• Unexpected IT demand, either high or low, due to errors in forecasting business operations • Merger and acquisition activities • Global and regional economic and political events

Source: IDC, 2002

Planned downtime is an increasing threat to business continuity because many businesses operate continuously or nearly continuously. While evenings and weekends have traditionally been a time when systems could be taken down without consequence, today's ecommerce applications extend the concept of "business hours" to 24 x 7.

Planned downtime is needed for routine maintenance activities. For example, a server needs additional attached-storage capacity or upgraded processors. Operating systems require upgrades, and application software must be enhanced and modified to keep it in alignment with business processes. The venerable backup-and-restore of data is most easily accomplished when production systems are quiescent.

Business volatility adds a third dimension to BCP. IT professionals and their line-of-business colleagues struggle to forecast accurately what demands marketplace behavior will place on IT systems. Errors are costly in either direction, as follows:

- Overly optimistic business forecasts encourage IT planners to increase capacity. When business lags, IT investments are underutilized and the total cost of ownership (TCO) rises proportionally.
- Pessimistic business forecasts lead to smaller investments in IT systems. When business booms, IT becomes a limiting factor, opportunity costs are incurred due to lost business, and TCO rises.

In summary, the major challenges for BCP are mitigating the risks of system downtime and business volatility with a set of countermeasures.

CASE STUDY: BUSINESS WIRE

Business Wire is a news service that distributes press releases from corporations to major media throughout the United States as well as globally. Business Wire's corporate clients depend on the company to provide timely, reliable, widespread distribution of information to investors, such as earning reports, press releases, and announcements of mergers and acquisitions. Business Wire maintains datacenters in New York City and San Francisco.

Steve Messick is the vice president for information systems at Business Wire. Messick led an effort beginning in 2000 to redesign the core systems at Business Wire to be resilient to site outages. The prior system, originally developed in the mid-1980s, was based on custom software written and maintained by Business Wire. Messick's objective was to move away from a home-grown solution and in the direction of industry-standard packaged solutions. A request for proposal was circulated, and HP emerged as the vendor of choice.

"HP understood our challenges," Messick said. "They showed us the components that we needed — processors and highly available storage and system management software — and they explained how the components would work together and remain resilient in the face of different risks." HP suggested the xp512 storage system, which provides highly available storage within a datacenter. For sitewide outages, HP recommended an asynchronous link using Continuous Access Extension XP between the primary datacenter in San Francisco and the secondary datacenter in New York. HP's MC/Serviceguard and Continentalclusters provide distant mirroring to the New York site as well as monitoring at the primary site to indicate when failover may be necessary. Should the San Francisco center become unavailable, the New York facility will take over the load in about 15 minutes.

HP provided consulting services to accelerate deployment. "We wanted to move very quickly. HP engineers assisted in the design and configuration of the system, which went into operation in about six months," Messick said. "We wanted a complete solution from a single supplier, and HP was able to provide exactly that."

Messick believes that Business Wire will continue to improve system resiliency over the coming months and also find more ways to exploit the advantages of its new primary/secondary datacenter model. "We see available resources in New York that we want to put to greater use for testing and other development work," he said.

Countermeasures

Countermeasures can be divided broadly into three approaches: techniques that decrease the likelihood that IT systems will fail, plans that accelerate recovery when IT systems do fail, and designs for adaptable infrastructure that delivers "just-in-time" provisioning of storage services. All three approaches are essential to a comprehensive business continuity plan.

Avoiding System Failure

Systems designed to be highly available are built with redundant components.

Systems designed to be highly available are built with redundant components. An engineer who knows the mean time between failure for subsystems, such as power supplies and magnetic disk drives, can improve reliability dramatically by using two or more of each critical component. If one power supply fails, then the second one takes over operation. Designers provide hot-swap capabilities so that the failed component can be replaced without taking down the system.

Intelligent storage systems can automatically detect that errors may soon begin appearing and proactively copy data over to another device before data loss actually occurs.

Within the datacenter, processing and storage recovery is provided by failover and redundant arrays of independent disks (RAID) techniques, respectively. Clustered servers can failover to others and keep the applications in operation. Data (including the application execution software) stored in a SAN can be redirected to the alternate server. For storage systems, the technology is based on the RAID. Failed disk drives can be hot-swapped and their contents rebuilt from the remaining disks. Intelligent storage systems can automatically detect that errors may soon begin appearing and proactively copy data over to another device before data loss actually occurs.

Redundancy is also a strategy for sources of power, network connections, and even for IT staffing. When possible, facilities planners can locate a datacenter so that enterprise networks have multiple, independent connections to the Internet. Similarly, facilities can be located to tap into two different power grids or designed with local power generation capabilities.

Well-documented procedures and staff cross-training reduce the risk of a human single point of failure.

Well-documented procedures and staff cross-training reduce the risk of a human single point of failure. In addition to skill sets, the BCP should specify that communication methods and equipment be available in support of alternate teams of professionals. Providing alternative methods of communication is particularly important because these systems come under severe loads in times of disaster. Plans for security are important to avoid tampering with systems and also to reduce human error.

Using new nondisruptive techniques can reduce scheduled downtime. Storage systems, for example, have point-in-time copy capabilities. While business applications continue to read and update data, a replica of that data can be split off and used for other purposes. Backup windows can be completely eliminated by using the point-in-time copies as source files for tape backups. These point-in-time copies may also be used to test a new version of the business application for stability and to verify performance.

CASE STUDY: TELUS

TELUS Corp. is one of Canada's leading providers of data, IP, voice and wireless communications services. TELUS provides and integrates a full range of communications products and services that connect Canadians to the world.

Rob Bolivar is manager of enterprise system solutions at the TELUS datacenters in Edmonton, Alberta. A primary focus of Bolivar's attention is an SAP transactional system that handles all of TELUS's internal support and supplies products to serve its customers.

"Access to critical services and support for our estores must be readily available," Bolivar said. TELUS estimates the direct cost of downtime to be $94,214 per hour. "This cost is directly related to the number of TELUS staff that cannot do their work if there were a system outage," Bolivar said. Other indirect costs, such as the ability to ship material and deploy technicians, would make this cost even higher.

The heart of TELUS's business continuance plan is a pair of datacenters located several kilometers apart. Initially, the SAP application was engineered to run at each of the datacenters. Data is mirrored between centers, and, even in the event of a centerwide failure, all of the SAP processing is transferred to the alternate site. Regular testing indicates that failover takes about 20 minutes, which is an acceptable time period for TELUS operations.

Using the SAP design as a model, Bolivar's staff has pushed business continuance plans into other key IT systems. Email, for example, is replicated between datacenters with Exchange servers running at each site. Business processes and IT staff skills are divided between the sites as well.

"HP has been a partner throughout the business continuity process," Bolivar said. "Their expertise with SAP was an important contribution early on. Products like MC/Serviceguard are key components in our datacenters. We use Information Technology Outsourcing (ITO) monitoring services from HP on an ongoing basis. ITO has become our sentinel for what is going on in our IT environments."

While concerns about disaster recovery and business continuity were primary objectives for IT managers at TELUS, Bolivar cites other unexpected advantages of the dual datacenter approach. With the ability to failover processing to the secondary datacenter, upgrades can be loaded and tested as needed at the primary datacenter. When the upgrade process is finished, Bolivar and his staff could failback and resynch the data. According to Bolivar, the new design provides "unbelievable flexibility." With the use of HP's Omniback product line, backup-and-restore procedures can be accomplished without taking systems out of service. "The unexpected benefits have made our lives easier," Bolivar said. "IT operations are smoother now that we have the dual datacenters in operation."

Accelerating Recovery

Disaster recovery plans begin with the assumption that an entire datacenter is no longer available and that the enterprise must turn to point-in-time backup copies, typically employing tape backup solutions or more real-time replicas of corporate data utilizing server or disk-based replication solutions. How the recovery proceeds depends on the distance to the backup datacenter and the replication method used, either synchronous or asynchronous.

Synchronous techniques are most often used to replicate data within a campus or metropolitan area or region, while asynchronous methods are used to replicate data over greater distances.

Distant data replication technologies. Distant data replication is an important BCP strategy for mitigating the risk of an outage affecting an entire datacenter (e.g., a fire, loss of power), or an even more widespread outage affecting all datacenters in a metropolitan area or region (e.g., an earthquake, a major storm). Synchronous techniques are most often used to replicate data within a campus or metropolitan area or region, while asynchronous methods are used to replicate data over greater distances.

Synchronous data replication. Data may be replicated by mirroring when datacenters are relatively close together. For storage and database systems that support OLTP applications, performance can be sustained for synchronous replication. Data can be stored locally and at a second datacenter while the OLTP monitor holds a transaction in suspense, and that transaction can be committed when acknowledgement is received from both the local and remote site.

The advantage of synchronous data replication is the speed and completeness of the recovery.

The advantage of synchronous data replication is the speed and completeness of the recovery. Should the primary datacenter suffer an outage, then all completed transactions are stored at the backup facility. Assuming that servers and application software are available, the failover from one datacenter to another can occur in seconds or minutes.

Asynchronous data replication. When data is replicated over hundreds or thousands of miles, asynchronous techniques are ordinarily needed. Asynchronous techniques are those that replicate data to a distant site, but there may be a temporary delay at times as data is transmitted. Transactions are committed locally without waiting for acknowledgement from the secondary site. Asynchronous techniques are needed because the effects of latency induced by the distance will cause too high a performance penalty.

Asynchronous techniques are also used when an application is not transactional in nature. A daily settlement process or a weekly market analysis procedure need not be replicated on a real-time, continuous basis. Copies should be transported to backup sites at checkpoints related to the application's calendar of usage.

An asynchronous approach to replication requires more analysis of the cost of downtime. For some applications, transmitting a daily point-in-time snapshot to the distant site combined with hourly transactional journals may provide sufficient system recovery time (e.g., a few hours to load the most recent snapshot and rebuild the transaction record).

In designing a distant data replication plan, the first concern of the enterprise should be in judging how far away a second site must be to avoid the risk of a single event affecting both centers. Distances of

BANDWIDTH AND LATENCY

Bandwidth is the throughput of a network — its capacity to move data as measured in bits per second. Latency is the time that it takes for data to move across a network from one location to another; it is measured in seconds.

Generally speaking, bits of data travel at a constant speed — the speed of light in optical fiber. Some latency is added when packets are processed by routers and forwarded to their destination.

While the speed of light may seem infinitely fast, over continental and global distances, latencies become a noticeable factor. Latency accrues in optical fiber at the rate of 2ms per 125mi round trip. The minimum latency for a U.S. coast-to-coast round trip (from datacenter A to datacenter B and back again) is 50ms; traveling halfway around the world and back in fibre takes about 200ms minimum.

For high-performance transaction processing systems, even a few milliseconds of additional delay may be unacceptable. An additional 200ms delay per transaction will affect performance significantly and may not be acceptable.

Latency is a particularly difficult challenge because, unlike bandwidth, spending more money cannot reduce latency. As our IDC colleague Chris Willard once said, "You can buy more bandwidth, but you can't buy less latency — you can't bribe God."

hundreds or thousands of miles will dictate an asynchronous solution. Next, planners must weigh two different objectives for recovery: the time to recovery and the recovery point. Both asynchronous and synchronous systems can be designed to return to service very quickly. The recovery point (i.e., the amount of processing that is lost) can be engineered for asynchronous replication techniques, which may lose some data.

Provisioning Storage

The flexibility of networked storage helps to address business continuity planning by routing consolidated data services to servers and edge devices on demand.

"Just-in-case" provisioning leads to lower utilization and higher costs.

Exhausting available storage capacity is a common threat to business continuity, particularly when storage is server-attached. This risk is often mitigated by over-provisioning — providing excess capacity just in case. Unfortunately, "just-in-case" provisioning leads to lower utilization and higher costs. In today's datacenter, however, storage can be consolidated and delivered just in time. Rather than over-provisioning, system designers can reprovision or reallocate storage quickly.

Provisioned, networked storage services, such as those provided by a SAN, can be rerouted when necessary. In the case of a server failure, for example, a backup server can be switched online without the need to move data to a new location. If a server that provides file or email services fails, then data can be rerouted to an alternative server.

CASE STUDY: CITY PUBLIC SERVICE, SAN ANTONIO, TEXAS

City Public Service of San Antonio, Texas, provides approximately 800,000 customers with electrical and natural gas services. In addition to monthly billing, account management also includes support for customer queries and reports of power outages. Billing information for several years is online and accessible.

When inclement weather causes power outages, the outage management system logs reports of outage, analyzes the outage pattern, and helps to dispatch repair crews. Quang Do is responsible for SAP-based systems at City Public Service. These systems are housed in two datacenters approximately three miles apart.

"We focused on our business requirements, and HP translated those requirements into a complete, working solution," Do said. "They helped us to design and install the systems." HP xp512 storage systems are in place at both facilities. HP's Metrocluster and MC/Serviceguard products provide high-system availability for both local and remote failover to backup hardware.

To replicate data both locally and remotely between the two centers in this environment, HP also supplies its xp512 products called Business Copy XP and Continuous Access XP. Processing takes place at the primary site under normal circumstances. Failover occurs automatically in the case of a primary datacenter outage.

"In addition to protection from site outages, we find that we have a more flexible system," Do said. "Backing up data is much simpler. Testing new versions of software can be accomplished at our secondary site while the primary site handles production."

SERVICES APPROACHES TO BCP

Third-party providers of storage services can play a significant role for smaller and midsize enterprises that do not have multiple datacenters.

Third-party service providers can play a key role in assisting in the BCP process. Experienced consultants can guide the analysis (audit) and design stages and participate in implementation and testing. Third-party providers of storage services can play a significant role for smaller and midsize enterprises that do not have multiple datacenters. The advantages of third-party outsource providers are as follows:

- Greater competency than many organizations and may be able to provide skills that are entirely unavailable in the enterprise
- Economies of scale since infrastructure and personnel costs can be shared across many customers
- Improved objectivity in looking at an enterprise as external consultants with a perspective over many enterprises and their varying needs

Third-party providers can assist in each of the major phases of BCP implementation as follows:

- **Audit.** Consultants can assist in building an inventory of applications and assessing how critical they are to the organization and what levels of service are needed to support business processes. Specialists with industry and cross-enterprise experience know the costs of downtime associated with different kinds of application and are aware of which applications typically show volatility.
- **Design.** Consultants can help enterprises design appropriate BCP systems and processes. A thoughtful design will reflect detailed enterprise knowledge of the impact of information systems on critical business processes and a thorough understanding of storage technologies, such as distant replication options.
- **Implementation.** Outsourced service providers can be useful partners as the enterprise IT staff engage in the BCP implementation process. The business model for outsource providers is based on providing shared services to a large group of customers. Economies of scale allow each customer to tap into expertise needed without incurring the costs of fielding a dedicated BCP staff.
- **Operations.** Rather than developing an alternative storage site, it may be more cost effective to subscribe to third-party storage services. Among other challenges, the storage service provider can address the issues of remote replication or provide a professionally managed backup/restore operation. For smaller and midsize enterprises, a storage service provider will likely provide a significant cost advantage over in-house efforts.
- **Monitoring.** Business continuity plans require regular testing. A mix of scheduled and unscheduled tests along with regular recurring audits are needed to make sure that the risk profile for the enterprise has not shifted. Systems must be reassessed and designs revisited to make sure that continuity plans are effective and to assess the opportunities that new technologies will provide.

CONCLUSION

Increasing dependence on information systems dictates that enterprises should have business continuity plans in place. Central to those business continuity plans will be the deployment of technologies and procedures that ensure the safety of data and the availability and recoverability of critical systems and applications. The magnitude of an enterprise's investment in data protection and disaster recovery will depend on the cost of downtime. Many enterprises will find it effective to contract with outsource service providers for some steps of the business continuity plan.

IDC Worldwide Offices

CORPORATE HEADQUARTERS

IDC
5 Speen Street
Framingham, MA 01701
United States
508.872.8200

NORTH AMERICA

IDC Canada
36 Toronto Street, Suite 950
Toronto, Ontario M5C 2C5 Canada
416.369.0033

IDC California (Irvine)
18831 Von Karmen Avenue
Suite 200
Irvine, CA 92612
949.250.1960

IDC California (Mountain View)
2131 Landings Drive
Mountain View, CA 94043
650.691.0500

IDC New Jersey
75 Broad Street, 2nd Floor
Red Bank, NJ 07701
732.842.0791

IDC New York
2 Park Avenue
Suite 1505
New York, NY 10016
212.726.0900

IDC Texas
100 Congress Avenue
Suite 2000
Austin, TX 78701
512.469.6333

IDC Virginia
8304 Professional Hill Drive
Fairfax, VA 22031
703.280.5161

EUROPE

IDC Austria
c/o Loisel, Spiel, Zach Consulting
Mayerhofgasse 6
Vienna A-1040, Austria
43.1.50.50.900

IDC Benelux (Belgium)
Boulevard Saint Michel 47
1040 Brussels, Belgium
32.2.737.76.02

IDC Denmark
Omøgade 8
Postbox 2609
2100 Copenhagen, Denmark
45.39.16.2222

IDC Finland
Jarrumiehenkatu2
FIN- 00520 Helsinki
Finland
358.9.8770.466

IDC France
Immeuble La Fayette 2
Place des Vosges Cedex 65
92051 Paris la Defense 5, France
33.1.49.04.8000

IDC Germany
Nibelungenplatz 3, 11th Floor
60318 Frankfurt, Germany
49.69.90.50.20

IDC Italy
Viale Monza, 14
20127 Milan, Italy
39.02.28457.1

IDC Netherlands
A. Fokkerweg 1
Amsterdam1059 CM, Netherlands
31.20.6692.721

IDC Portugal
c/o Ponto de Convergancia SA
Av. Antonio Serpa 36 - 9th Floor
1050-027 Lisbon, Portugal
351.21.796.5487

IDC Spain
Fortuny 18, Planta 5
28010 — Madrid
Spain
34.91.787.2150

IDC Sweden
Box 1096
Kistagangen 21
S-164 25 Kista, Sweden
46.8.751.0415

IDC U.K.
British Standards House
389 Chiswick High Road
London W4 4AE United Kingdom
44.208.987.7100

LATIN AMERICA

IDC Latin America
Regional Headquarters
8200 NW 41 Street, Suite 300
Miami, FL 33166
305.267.2616

IDC Argentina
Trends Consulting
Rivadavia 413, Piso 4, Oficina 6
C1002AAC, Buenos Aires, Argentina
54.11.4343.8899

IDC Brazil
Alameda Ribeirao Preto, 130
Conjunto 41
Sao Paulo, SP CEP: 01331-000 Brazil
55.11. 3371.0000

International Data Corp. Chile
Luis Thayer Ojeda 166 Piso 13
Providencia
Santiago, 9, Chile
56.2.334.1826

IDC Colombia
Carerra 40 105A-12
Bogota, Colombia
571.533.2326

IDC Mexico
Select-IDC
Av. Nuevo Leon No. 54 Desp. 501
Col. Hipodromo Condesa
C.P. 06100, Mexico
525.256.1426

IDC Venezuela
Calle Guaicaipuro
Torre Alianza, 6 Piso, 6D
El Rosal
Caracas, Venezuela
58.2.951.1109

CENTRAL AND EASTERN EUROPE

IDC CEMA
Central and Eastern
European Headquarters
Male Namesti 13
110 00 Praha 1
Czech Republic
420.2.2142.3140

IDC Croatia
Srednjaci 8
1000 Zagreb
Croatia
385.1.3040050

IDC Hungary
Nador utca 23
5th Floor
H-1051 Budapest. Hungary
36.1.473.2370

IDC Poland
Czapli 31A
02-781 Warszawa, Poland
48.22.7540518

IDC Russia
Suites 341-342
Orlikov Pereulok 5
Moscow, Russia 107996
7.095.975.0042

MIDDLE EAST AND AFRICA

IDC Middle East
1001 Al Ettihad Building
Port Saeed
P.O. Box 41856
Dubai, United Arab Emirates
971.4.295.2668

IDC Israel
4 Gershon Street
Tel Aviv 67017, Israel
972.3.561.1660

IDC South Africa
c/o BMI TechKnowledge
3rd Floor
356 Rivonia Boulevard
P.O. Box 4603
Rivonia 2128, South Africa
27.11.803.6412

IDC Turkey
Tevfik Erdonmez Sok. 2/1 Gul
Apt. Kat 9D
46 Esentepe 80280
Istanbul, Turkey
90.212.275.0995

ASIA/PACIFIC

IDC Singapore
Asia/Pacific Headquarters
80 Anson Road
#38-00 IBM Towers
Singapore 079907
65.6226.0330

IDC Australia
Level 3, 157 Walker Street
North Sydney, NSW 2060
Australia
61.2.9922.5300

IDC China
Room 611, Beijing Times Square
88 West Chang'an Avenue
Beijing 100031
People's Republic of China
86.10.8391.3610

IDC Hong Kong
12/F, St. John's Building
33 Garden Road
Central, Hong Kong
852.2530.3831

IDC India Limited
Cyber House
B-35, Sector 32, Institutional
Gurgaon 122002
Haryana India
91.124.6381673

IDC Indonesia
Suite 40, 17th Floor
Jakarta Stock Exchange
Tower 2, Jl. Jend. Sudirman Kav. 52-53
Jakarta 12190
6.221.515.7676

IDC Market Research (M) Sdn Bhd
Jakarta Stock Exchange Tower II
17th Floor
Jl. Jend. Sudirman Kav. 52-53
Jakarta 12190
62.21.515.7676

IDC Japan
The Itoyama Tower 10F
3-7-18 Mita, Minato-ku
Tokyo 108-0073, Japan
81.3.5440.3400

IDC Korea Ltd.
Suite 704, Korea Trade Center
159-1, Samsung-Dong
Kangnam-Ku, Seoul, Korea, 135-729
822.551.4380

IDC Market Research (M) Sdn Bhd
Suite 13-03, Level 13
Menara HLA
3, Jalan Kia Peng
50450 Kuala Lumpur, Malaysia
60.3.2163.3715

IDC New Zealand
Level 7, 246 Queen Street
Auckland, New Zealand
64.9.309.8252

IDC Philippines
703-705 SEDCCO I Bldg.
120 Rada cor. Legaspi Streets
Legaspi Village, Makati City
Philippines 1200
632. 867.2288

IDC Taiwan Ltd.
10F, 31 Jen-Ai Road, Sec. 4
Taipei 106
Taiwan, R.O.C.
886.2.2731.7288

IDC Thailand
27 AR building
Soi Charoen Nakorn 14,
Charoen Nakorn Rd., Klongtonsai
Klongsan, Bangkok 10600
Thailand
66.02.439.4591.2

IDC Vietnam
Saigon Trade Centre
37 Ton Duc Thang Street
Unit 1606, District-1
Hochiminh City, Vietnam
84.8.910.1233; 5

IDC is the foremost global market intelligence and advisory firm helping clients gain insight into technology and ebusiness trends to develop sound business strategies. Using a combination of rigorous primary research, in-depth analysis, and client interaction, IDC forecasts worldwide markets and trends to deliver dependable service and client advice. More than 700 analysts in 43 countries provide global research with local content. IDC's customers comprise the world's leading IT suppliers, IT organizations, ebusiness companies and the financial community. Additional information can be found at www.idc.com.

IDC is a division of IDG, the world's leading IT media, research and exposition company.

02-072STORAG3408
July 2002

IDC
Analyze the Future

www.idc.com