DPRO-100862
Kristen Noakes-Fry,
Trude Diamond

Technology Overview
12 September 2001

Business Continuity Planning and Management: Perspective

Summary

Gartner research conducted in 2000 found that over 60 percent of IT managers surveyed did not believe their companies had a basic continuity plan to mitigate the effects of a disaster. Such disasters that disrupt business can run the gamut from natural disasters to the myriad risks inherent in dependence upon technology for all aspects of operation. The challenge is, first, to assess the costs of the risks facing a company, and then develop a plan to avoid, mitigate, and (at worst) recover rapidly from any level of business disruption— from inconvenience to full-fledged disaster. For enterprises in need of enhanced business continuity plans (BCPs) and resources, help is available. The questions are these: Which kind of help best fits each company's needs? And for each kind of help, should the company build and maintain the solution or contract for services it can access when needed? Answering these questions requires understanding the services that support making business continuity (BC) decisions and selecting products and services for outsourcing any (or all) elements of the continuity strategy.

Table of Contents

List Of Tables

Technology Basics

The Need for Business Continuity Planning and Management (BCPM)

With the growth of e-commerce and other factors driving system availability expectations toward 24x365, the average organization's requirement for recovery time from a major system outage has come to range between two and 24 hours. Companies are striving to meet the demand for continuity. Business survival necessitates planning for every type of business disruption— including, but by no means limited to— the categories of natural disasters, hardware and communications failures, internal or external sabotage, and the failures of supply chain and sales affiliate organizations. Such disruptions cannot be predicted but can wreak havoc upon the business, with results ranging from insured losses of replaceable tangibles to uninsurable capital losses, to customer dissatisfaction and possible desertion, to complete insolvency. Perhaps the most important point to make about BC support technologies is that its effectiveness depends entirely upon the enterprise's commitment to the entire project, including the updating and testing necessary for maintenance.

With corporate risk management coming under increasing scrutiny in the aftermath of recent natural disasters and e-business technology failures, **business continuity planning**— the result of which is called **business continuity management**— satisfies many of the evolving demands upon companies.

- Customers expect supplies and services to continue— or resume rapidly— in all situations. Shareholders expect management control to remain operational through any crisis.
- Employees expect their lives and livelihoods to be protected, and suppliers expect the same of their revenue streams.
- Regulatory agencies expect their requirements to be met, regardless of circumstances.

A business continuity strategy, then, is a high-value— but high-maintenance— proposition. Business continuity embraces a broad spectrum of technologies: old and new, paper based and electronic, manual and automated, individual and integrated. The key challenge of BCPM is not technology, however, but the internal marketing "business" aspects that begin at the foundation level of any project and continue throughout its life cycle: justification, executive buy-in, broad organizational support, and governance and politics. A business continuity management plan, adequately supported throughout the enterprise, embodies the strategic framework for a corporate culture that embraces a variety of tactics to mitigate risks that might cause:

- Business process failure
- Asset loss
- Regulatory liability
- Customer service failure
- Reputation or brand damage

Solid requirements engineering for any project begins with the fundamental question: What does the business need? Business continuity planning is no exception. The first place to ask that question is at the level of enterprise strategic plans and policies. Projects, particularly ones like continuity planning that span operational and support units, must align closely with broad, strategic objectives and have clear executive sponsorship for the projects' critical support of those strategies.

Business Continuity Planning and Management: Perspective

The Phases of Business Continuity Planning, Implementation, and Management

The significance of each major phase of continuity planning merits attention because each phase contributes to building all four areas of business continuity: disaster recovery, business recovery, business resumption, and contingency planning.

- **Phase 1— Establish the foundation.** These alignment and analysis steps are necessary to obtain executive sponsorship and the commitment of resources from all stakeholders. Without the Business Impact Analysis and Risk Assessment basis, the plan cannot succeed and may not even be developed.
- **Phase 2— Develop and implement the plan.** Here, attention to detail and active participation by all stakeholders ensure the development of a plan worth implementing. The plan itself must include the Recovery Strategy with all of its detailed components and the Test Plan.
- **Phase 3— Maintain the plan**. The best plan is only as effective as it is current. Every tactic of business resumption and recovery must be kept up to date and tested regularly.

Service Options

One significant trend among BCPM service vendors is to focus on business continuity as a whole. Recovery itself must be speedy (under 24 hours) for high-availability systems— and the facilities must provide continuity not only of the data center (the "glass house"), but also of all critical aspects of its clients' businesses. This focus provides clients a more integrated service while allowing the vendor to maintain better account control.

Consulting Assistance

- **Software and Consulting.** Many service providers offer combinations of tactical consulting with business continuity planning and management software, sometimes including full continuity management services and hot-site facilities.
- **Hardware and Consulting.** Hardware vendors may combine continuity planning consultancy with rapid hardware replacement shipment, mobile-site delivery, or hot-site facilities.
- **Internet E-Commerce Continuity and Consulting.** Communications and networking vendors may offer high-availability networking and rapid recovery solutions with tactical consulting.
- **Product-Independent Consulting.** Consultants who provide analyses, audits, and tactical recommendations based upon such studies offer objectivity in the development of the specifications a company should use to select business continuity products and services.

Hot Sites, Cold Sites, and Off-Site Data Storage

Stand-alone considerations for off-site recovery remain a significant part of the continuity management strategy. Specific types of service may be combined to provide the exact package any company specifies.

- **Hot Site.** A hot site is an operationally ready data center offering specific hardware platforms for near immediate availability when notified of a disaster. Standard availability was once measured in days; with e-business driving requirements today, however, hot sites are providing (for a cost) options that provide availability within hours. Subscriptions are based on the hardware specifications required to recover a "like" computer configuration. Subscriptions average 40 months' duration; cost from hundreds to hundreds of *thousands* of dollars (U.S.) per month, depending upon the company's requirements; and allow hot-site use for up to eight weeks in disaster mode.

- **Cold Site.** An empty, environmentally conditioned computer room available on a subscription basis, ranging from 12 to 60 months and costing between $500 and $2,000 per month. Hot-site providers generally include this service in the basic cost of a hot site for use after the subscriber has exceeded its occupancy time at the hot site.
- **Off-Site Storage.** Depending on budget and geographical risks, off-site storage for backup data on tape or disk could be the building next door, a bank safety deposit box, or the branch office across town. A better choice is a secure, climate-controlled, fireproof media vault at a storage facility maintained by a commercial media storage provider. At higher cost, some vendors offer a service level of storage providing media that can quickly become live— sometimes called "electronic vaulting." Companies must ensure that contractually defined accessibility of the off-site copy meets original requirements, as for all outsourced elements of the business continuity solution.
- **Mobile Site or Porta-Site.** Mobile computer/office environments available for smaller hardware configurations or emergency office environments. **Mobile sites** are stand-alone units on mobile trailers. **Porta-sites** are transported to the facility and constructed on-site. These options cost essentially the same as cold sites. Mobile hot sites have been increasing in popularity because they bring the work area to the end user.
- **OEM Insurance.** Hardware companies may offer a form of insurance guaranteeing that they will replace damaged computer equipment with a system of equal or greater processing capacity within a specified period of time. The insurance cost is usually six to eight percent of the monthly maintenance bill.
- **Quick Ship.** Most third-party leasing vendors provide guaranteed rapid shipment of replacement hardware as a recovery option. Customers pay a priority equipment search fee and the normal leasing charges plus a premium when they request shipment.
- **PC-Based Planning Tools.** Virtually all hot-site vendors offer some form of PC-based disaster recovery plan development tool. In many cases (like consulting services), these packages are provided to a client organization as an enticement to acquire its hot-site services.
- **Advanced Recovery Services.** Sometimes called "electronic vaulting" of data from the subscriber site to the hot site. This costly service requires that a direct-access storage device (DASD) be dedicated to the subscriber, preventing the service from being shared with other subscribers. PC/LAN electronic data vaulting is emerging as a popular service.

Technology Analysis

Business Use

Every industry depends increasingly on integrated systems, yet surveys have shown that nearly one-third of enterprises have no manual alternatives to fall back on during a technological disruption. The need for high availability of systems today approaches 24x365 across all industries, for both service and manufacturing organizations. Despite that fact, the relatively high percentage of companies without business continuity plans indicates that strategic planners may be relying on a combination of insurance and outsourced physical recovery sites to take the required steps independently, absent any cohesive enterprisewide plan to coordinate activities. The concept of disaster recovery has expanded into **business continuity planning and management (BCPM)**. Recent demands for continuity services have resulted largely from crises caused by power outages, technology failures, human errors, and natural disasters. The types of continuity services most utilized include the following:

- Business operations recovery, including order intake, order fulfillment, customer service, and supply chain management.
- IT operations recovery.
- IT hardware replacement.

Traditionally, industries with the greatest need for business continuity planning and management have been government, health services, and finance, but continuity planning and management has penetrated large- to medium-size companies across all industries, and particularly in those attempting compliance with the International Organization for Standardization (ISO) standards or required to comply with industry regulation. Government entities; retailers with e-commerce channels; and the finance (banking, securities, and insurance), health, and regulated utilities industries currently use BCPM products and services most heavily— particularly those of *Fortune* 1000 size. Increasing reliance on e-business has added retailers with e-commerce channels, along with Internet service providers (ISPs) and application service providers (ASPs), to this user group.

Government

Federal regulatory legislation drives much industrial use of BCPM services. Governmental self-regulation to ensure continuity of all operations and services underwent heavy scrutiny during Y2K systems preparedness efforts. What probably contributed to the uneventful continuity of federal services through the Y2K episode was the array of Continuity of Operations Planning (COOP) Office of Management and Budget (OMB) circulars and presidential directives driving risk management for all federal agencies. Every U.S. Federal department and agency has taken BCPM measures in accord with the COOP directives. All U.S. state governments and national governments worldwide have in place ongoing efforts to establish and expand continuity planning and management resources.

E-Commerce

E-tailers, ISPs, and ASPs have learned about the vulnerability of the Internet and e-commerce to business disruptions from the recent attacks suffered by prominent e-commerce companies such as Yahoo, eBay, CCN News, and American On-line. These attacks come as e-business grows increasingly dependent on the reliability and availability demands by customers for online 24x365 service operations. Every major provider of business continuity resources now offers high-availability e-commerce recovery services at commercial hot sites.

Finance

In the U.S., the Gramm-Leach-Bliley Act, the Expedited Funds Availability Act, and SAS70 audit reports require effective business continuity plans and resources. The *FDIC Comptroller*'s Handbook requires national banks to include restoration of the Internet banking channel among the regularly tested elements of their business continuity plans. The U.K. Financial Services Act and similar legislation in most nations put forth comparable requirements. Even without regulation, the finance industry would have strong bottom-line motivation to avoid business disruption. For a bank, the cost of service interruption has been estimated at between $60,000 and $250,000 a minute, according to industry sources, and the average bank computer loss has been estimated at $1.5 million.

Health

Health-related businesses have always secured resources for ensuring the availability of service in the face of disruptive events. Since Congress adopted the Health Insurance Portability and Accountability Act (HIPAA) in 1996, the U.S. health industry (healthcare plans, providers, and clearinghouses) has also had

to implement standardized electronic claims and payment systems. Those systems became folded into existing continuity strategies and spurred even greater development of well-managed plans and recovery resources.

Regulated Utilities

The continuity of power, telecommunications, and water utilities is a critical assumption of the continuity plans for other public services (hospitals, police, fire/rescue, schools and other designated "shelters," and government offices) and large or regulated business and services (banks, insurance companies, brokerages, Internet communications services). The U.S. Federal Communications Commission (FCC) oversees coordinated network service continuity planning by telecommunications carriers and other providers of telecommunications service. The U.S. Environmental Protection Agency (EPA) enforces many environmental regulations, including its provisions for BCPM, to ensure the availability of safe power and water supplies and services despite disruption scenarios. State Departments of Environmental Services and Public Utilities Commissions (in some states called Public Services Commissions) oversee enforcement of state Public Utilities Code legislation ensuring reliability (continuity) of business and service. In other countries, national and regional governmental agencies enforce similar legislation requiring plans for continuity of critical infrastructure services after disruptive emergencies. As these entities' operations continuity needs have expanded into total business continuity, so have their plans and the software infrastructure supporting the plans themselves.

Benefits and Risks

Benefits

BCPM support can provide specific expertise and services that ensure a company's capability to cost effectively maintain operations despite a crisis. Each corporation must determine the appropriate types and service levels it requires from the array available: full-service consultancies, continuity service vendors, and software that perform a spectrum of services from continuity plan development to communication and maintenance. Once the necessary types of support have been selected, the BCPM solution should present substantial benefits.

Development and Maintenance of a Reliable Plan Structure

Using elements of BCPM consultancy, recovery sites, and supporting software demonstrates conscientious attention to best practices for thorough planning.

Efficient Resource Commitment and Task Allocation

Ensuring a full complement of resources to plan implementation, including testing through worst-case scenario drills, satisfies the demands of both shareholders and auditors.

Reliable, Accurate Plan Notification and Distribution

Integrating the plan's "calling tree" database into the corporate employee contact information database guarantees that the right parties receive each type of notification, with a minimum of database maintenance effort. Periodic tests ensure accuracy.

Thorough Plan Management Reporting

Version tracking is important to the risk management team, and periodic snapshots of the entire plan or elements of it are necessary for business functions such as budgeting, staffing, and competitive analysis.

Risks

Business Continuity Planning and Management: Perspective

All plans— even scrupulously developed, rigorously tested, automatically distributed, accountably executable plans— "rust." Without continuous process improvement procedures in place for periodic plan review and event-triggered plan reviews to reflect changes in the enterprise, the baseline continuity plan will rapidly become obsolete. The risk management team must be vigilant against some of the risks in using BCPM software.

Even among corporations with business continuity plans, a KPMG study shows that less than one-half meet an acceptable portion of their recovery objectives. The business infrastructure seems to be less protected than its stewards think it is, and such surprises usually lie in failure to tend the corporate domain. Two curable causes of disappointing continuity plan performance may be viewed as "spotty plans" and "plan rust." Spotty plans suffer from gaps either in the initial continuity plan or in the current plan's rust from lack of exercise (testing).

Over-Reliance on Support— Consultants, Recovery Services, and Software

While all industry-leading BCPM service vendors use time-tested, analytical tools, they also allow customization, and for good reason. As the company's staff interacts with consultants, outlines recovery strategies at secure sites, and completes structured BCPM templates, it should always be thinking, "What unique-to-us factor must we add?"

Neglecting Maintenance

Every responsible company has change management procedures, and continuity planning integrates logically into them. Decades of industry experience have proven that the BCP that lies forgotten in a desk drawer is of little practical use in a real emergency.

Consultant or Vendor Reliability and Contracting Issues

Perform due diligence as required for any major purchase to ensure that the consultant or the vendor of recovery services or of BCPM software has a good reputation for support of its embedded client base. Be sure to review the service contract with an attorney well acquainted with such contracts and the unseen pitfalls that may be present in the "standard" contract (for example, automatic renewal clauses).

Standards

International, Cross-Industry Standards

ISO/International Electrotechnical Commission (IEC) 17799:2000

ISO/IEC 17799:2000, 2000 *Information Technology— Code of practice for information security management*, an international version of British Standard 7799-1:1999, was published in December 2000. It contains 10 major sections, one of which is business continuity management (Section 11). However, parts of Physical and Environmental Security (7), Asset Classification and Control (5), and Security Policy (3) would also apply.

ISO/IEC Technical Report (TR) 13335

ISO/IEC Technical Report (TR) 13335, *Guidelines for the Management of IT Security* (*GMITS*), 13335-2: *Managing and Planning IT Security*, contains requirements for procedural security, including business continuity.

ISO 9002

This quality assurance model applies to organizations that produce, install, and service products. It implies industry standards for IT Security and the broader subject of general product security, including

continuity planning for IT systems— both as products themselves and as environmental support— and all other aspects of business operations (physical, environmental, personnel) whose disruption would affect product security.

National Institute of Standards and Technology (NIST) Special Publications (SP) 800 Series

NIST Special Publications (SP) 800 Series (parts 3, 4, 12, 14, 16, and 18) require contingency, disaster recovery, and continuity of operations plans.

Industry-Specific Standards and Regulations

Regulatory compliance can play a major role in motivating companies to implement thorough business continuity plans.

U.S. Federal Government

Government agencies with essential missions at federal, state, and local levels have always had continuity plans. The Continuity of Operations Planning (COOP) directives produced by the Office of Management and Budget (OMB) and the President of the United States outline the objectives of business continuity planning for all federal departments and agencies. Examples are as follows:

- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," published in 1993, ensures that appropriate business continuity plans were put in place for all Federal general-purpose systems and major applications, which include the mission-critical applications identified under the Y2K program.
- Presidential Decision Directive (PDD) 67, issued 21 October 1998, requires Federal agencies to develop Continuity of Operations Plans for Essential Operations.
- Executive Order 12656 [Section 202] requires the head of each Federal department and agency to ensure the continuity of essential functions in national security emergencies by providing for safekeeping of essential resources, facilities, and records and establishment of emergency operating capabilities.
- Presidential Decision Directive (PDD) 63, issued in May 1998, calls for a national effort to ensure the security of the United States' critical infrastructures— the physical and cyber-based systems essential to the minimum operations of the economy and government. It sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003 and requires the Federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained.

Finance

- **Gramm-Leach-Bliley Act** of 1999, Section 501(b) Financial Institutions Safeguards, requires that the agencies described in Section 505(a) establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards for the security and confidentiality of customer records and information. The compliance deadline for this legislation was 1 July 2001.
- **The Expedited Funds Availability Act** enacted by the U.S. Controller of Currency (1 January 1989) required federally chartered financial institutions to have a demonstrable business continuity plan to ensure prompt availability of funds.

- **SAS70 reports**, in accord with a statement on Auditing Standards Number 70 issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) in 1993, review the processing of transactions by service organizations, such as electronic data processing (EDP) centers and banks. SAS70 reports must be performed by certified external auditors, who examine general computer controls, qualified service providers, participant eligibility, and claim system application controls and review the findings with management.

Health

HIPAA— In 1996 the U.S. Congress adopted the Health Insurance Portability and Accountability Act (HIPAA), requiring healthcare plans, providers, and clearinghouses to adopt standardized electronic claims and payment systems. Noncompliance fines start at $100 for failure to meet a standard, but range up to $250,000 and 10 years' imprisonment for the wrongful use or disclosure of individual health information for commercial advantage, personal gain, and the like. Also, accreditation agencies, such as the Joint Commission on Accreditation of Health Care Organizations (JCAHO) inspect for compliance during their accreditation process.

Utilities

The Telecommunications Act of 1996, Section 256, "Coordination for Interconnection" requires the Federal Communications Commission to establish procedures to oversee coordinated network planning by telecommunications carriers and other providers of telecommunications service. It also permits the FCC to participate in the development of public network interconnectivity standards by appropriate industry standards-setting bodies. The act recognizes the need for disaster recovery plans, but also acknowledges the existence of inadequate testing because of the rapid deployment of new technologies.

Price vs. Performance

Who Pays for Business Continuity and Recovery— and How Much?

For a company to stay in business during a disruptive event and to continue in business in the months and years that follow require more than allocating a small percentage of the data center budget. On the average, around 4 percent of the data center budget is allocated to disaster recovery. However, it is not just the data center that is involved in business continuity. All essential departments and functions must continue to operate at something approaching normal productivity. Therefore, the cost of the enterprise business continuity program is best borne by all operational and support units that would benefit. If the continuity plan and implementation have been derived from enterprise strategic objectives and have executive sponsorship— particularly in corporations that fund at the strategic level instead of the project level— costs will be apportioned across all affected units.

Selection Guidelines

Each company's selection of a business continuity solution must use its unique impact and risk analyses as guidelines. The "best" solution for business continuity planning and management will consist of the right mix of internal controls and tools with outsourced services that will meet the company's requirements for managing physical, technological, legal, regulatory, and human resource aspects of business continuity. The initial solution will change over time, depending on the company's reliance upon technology, the existence of manual workarounds for technological failure, and each operation site's exposure to environmental risk factors like power outages and natural disasters.

Once identified, the components of the continuity solution range across the spectrum from fully internal to fully outsourced elements. Again, each company must determine its own best balance between full internal resources and their management, or management of some internal resources and some

outsourced services, or fully outsourced continuity management and resources. Each option has its apparent costs, as well as hidden costs— particularly the hidden costs of internal resource maintenance and management.

A decision process may include a variety of risk/value/cost considerations.

- Which business information, processes, and their supporting systems require 24x365 availability?
- What are the most likely disruptive occurrences at each corporate site?
- Which solutions are most readily available for each type of crisis?
- Which solutions for prevention and recovery meet the systems' availability demands cost effectively?

The Right Fit for the Shape of the Enterprise

Initiating a company's first integrated business continuity plan and managing it can be overwhelming. More importantly, the effort is usually beyond the expertise of the company's internal team charged with developing the plan. The best first decision may well be to select an experienced consultant to assist at least the start-up project. Such an advisor can provide insight into later decisions about which processes to maintain internally and which to outsource.

The Table "*BCPM Solution Development Process*" presents a potential path to follow.

Table 1: BCPM Solution Development Process

BCPM Issue	External Support Options
Phase 1: Develop the Foundation	
Is there executive support across all units of the enterprise?	• Advisement-only consultant • Consulting service from existing hardware vendor • BCP software for business impact analysis (BIA) and risk assessment (RA) with or without the software vendor's consulting service
Needs: • Business Impact Analysis • Risk Assessment **Considerations for Vendor Selection:** • Objectivity of internal assessment vs. external analyst • Account management motives of hardware and software vendors	**Deliverables:** • BIA report with values of all assets and costs of all disruption scenarios • RA report with risk/benefit analysis and continuity priorities
Phase 2: Develop the Plan	
Is there in-house expertise in continuity planning and management?	• Advisement-only consultant • Consulting service from existing hardware vendor • BCP software for BCPM with or without the software vendor's consulting service

Table 1: BCPM Solution Development Process	
BCPM Issue	**External Support Options**
Phase 1: Develop the Foundation	
Needs: • Business units' existing continuity plans (if any) • BCPM team member identification • Prioritization of continuity-targeted operations and systems • Comparison pricing among alternative solutions • Comparison pricing among competing vendors of each solution • Selection of resources for crisis prevention and rapid recovery • Allocation of funding for plan implementation and maintenance **Considerations for Vendor Selection:** • Extent of experience with BCPM in the same industry • Extent of experience with BCPM in similar environments (technical, physical, regional)	**Deliverables:** • Matrix of existing plans and recommended adoption of best practices • BCPM roles/responsibilities and call list • Operations and systems priority list • BCPM requirements (specifications for request for proposal [RFP]) • Solution cost comparison and recommendations • Vendor cost comparison and recommendations • RFP developed and sent to potential vendors • Vendor proposals evaluated and ranked for recommendation • Funding allocated for plan implementation and maintenance
Phase 3: Maintain the Plan	
Are there internal resources to carry out this effort?	• Advisement-only consultant • Consulting service from existing hardware vendor • BCP software for BCPM with or without the software vendor's consulting service
Needs: • Employee training on continuity procedures • Automated (or manual) update of plan resource lists to reflect current corporate data • Automated (or manual) notification of plan updates • Test trigger events and scheduled tests • Performance of triggered and scheduled tests • Evaluation of test results • Implementation of post-test plan updates **Considerations for Vendor Selection:** • Track record of success for crisis avoidance • Track record of success for rapid recovery (mean time to repair [MTTR] statistics) • Extent of experience in the same industry • Extent of experience in similar environments (technical, physical, regional)	**Deliverables:** • Continuity procedures employee training package • Methodology description for update of plan resource lists to reflect current corporate data • Methodology description for notification of plan updates • List of test trigger events and scheduled tests • Methodology description for performance of triggered and scheduled tests • Methodology description for test results evaluation • Methodology description for post-test plan update implementation

Technology Leaders

Initially, most vendors marketed their services as "hot sites" providing standby computer resources, in the event that one or more subscribers suffering a regional crisis required an alternative computer center to

process critical applications. The hot-site industry has successfully recovered hundreds of companies since its inception in the early 1980s. A large number of those recoveries resulted from regional events affecting multiple subscribers simultaneously, with no client ever having been denied access to a recovery facility because of excessive demand.

Today, vendors offer a broad spectrum of services for BCPM— continuity plan development and maintenance, and plan activity implementation and management, including disaster recovery. Their offerings have become increasingly comprehensive, with many vendors encompassing several aspects of business continuity.

Each company's unique requirements will determine its most appropriate BCPM vendor. Once an enterprise decides upon the degree of internal control and management of its business continuity process it wants to retain, it can identify the vendor with the best integration of the necessary advisement and implementation resources or several vendors whose coordination will be managed in-house.

The Table "*Vendors at a Glance*" lists those vendors supporting BCPM and reveals the kind of support that each provides.

Vendors at a Glance							
	Full-Service Consulting	**Management Services**	**BCP Software**	**Hot Sites***	**Cold Sites**	**Off-Site Data Storage**	**Hardware Quick Ship**
For Organizations Seeking Highly Outsourced Planning and Management Solutions:							
IBM	X	X		X	X	X	X
Comdisco**	X	X	X	X			
SunGard	X	X	X	X	X		
For Organizations Seeking Assistance With Continuity Planning, but Not Outsourced Management of Continuity/Recovery Resources:							
Strohl	X		X				
RSM McGladrey	X		X				
LBL Technology Partners	X		X				
Business Protection Systems	X		X				

*Hot sites include Internet/e-commerce recovery.

**By the end of 2001, Comdisco may be acquired by one of the other players in the BCPM arena.

Full-Service Vendors

Two different approaches characterize these providers of products and services. First, companies such as IBM developed broad recovery and then BCPM services to support the needs of its embedded base of hardware customers. IBM boasts decades of experience upon which its consulting services rely and characterizes its continuity offerings as "whatever it takes" to meet clients' requirements for recovery of

multi-platform systems. For “whatever it costs,” IBM certainly can provide the spectrum of products and services necessary to meet any client’s continuity objectives.

Comdisco and Sungard, on the other hand, began as business recovery service providers and expanded into the BCPM software business to capitalize on their 20+ years of experience. Where IBM uses proprietary methodologies to drive consistency in delivery of the expertise in its consulting services, Comdisco and Sungard sell their expert system software. This approach allows clients more latitude in self-management of the continuity planning process— from performing business impact and risk analyses, to completing (and custom-tailoring) a continuity plan template and managing the plan’s evolution.

Both approaches entice clients into expanded relationships with these service providers. Given the complexity of business continuity planning and management, and the “always something new” expertise required, that relationship may be as valuable to the client as it is to the vendor.

Continuity Planning Support Vendors

Strohl, RSM McGladrey, LBL Technology Partners, and Business Protection Systems provide primarily BCPM software and related planning advice that may be useful to small- to mid-size companies with existing IT recovery plans and the prudent objective of expanding business continuity throughout the enterprise. These plan-development tools enable such companies to perform initial assessments and create a plan that they can manage in-house— or outsource if its complexity turns out to be too cumbersome for internal resources.

Technology Alternatives

Much of the inescapable groundwork of BCPM is based in human “wet-ware”: people’s brains— not technology. Only a company’s employees can know the value of assets and their availability requirements. Taking the level of effort necessary to input that information into any of the technical solutions as a baseline, the choices become how much of the cost of BCPM to manage predictably through outsourced services and how much to “save” at the risk of partial or total operations failure.

Outsource Fully

The cost of using a fully outsourced solution is a predictable annual line item. The company’s team can experience minimal impact on its time from the additional task of acting as liaison with the service provider.

Insource Fully

The initial cost of continuity planning without professional advice or expert-system software may appear low, but even at that early stage hidden costs of unplanned employee time for plan research and revision can increase the budget by an order of magnitude. The downstream risks from building on an incomplete foundation can cause unpredictable budget overruns for playing catch-up instead of having a managed recovery after a disruption.

Have No Resources— Folly

Companies in the 10 percent that report having no continuity plan in place risk failure— one power outage and the customers jump to the competition. The issue for such companies is not mean time to recovery: it’s mean time to bankruptcy.

Insight

Business continuity planning and management is a core responsibility of every company, and more organizations are taking it seriously enough to seek professional assistance with developing solid continuity plans and managing them properly. One of the barriers— if not the major barrier to effective continuity planning— is the difficulty of obtaining executive sponsorship. The cost of continuity may be perceived as a payment made for a resource that is never used, one whose elements may appear to be covered by an array of separate, uncoordinated security features, and certainly one whose immediate return on investment (ROI) does not appear on the next quarter's outlook report. When funding follows enterprise strategy, the proponents of BCP can develop a clear cost justification that will attract executive sponsorship. Advisors can assist with baseline assessments and initial plan development. Service providers can manage the plan's implementation by providing physical off-site facilities for continuity immediately after a crisis and then delivering new hardware to the company's own site to restore operations there. Hired experts and their services can provide all the assistance a company requires. The critical resource that only the company itself can supply is *commitment* to keeping the plan current and testing the continuity tactics as often as needed.