Aftermath & Aftershocks:
A Gartner View

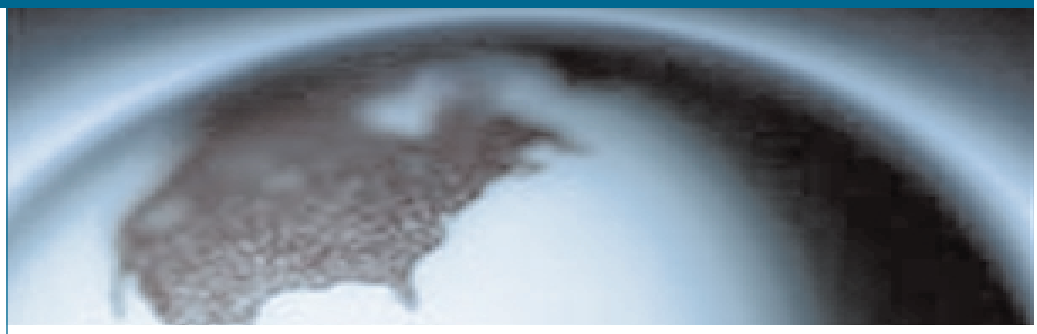


Table of Contents

Global Aftershocks: What the Attack on America Means

Letter from the Editor

26 September 2001

Like most Gartner analysts, I work from home. Less than a mile from Washington, D.C., I am becoming accustomed to the 24-hour-a-day roar of military jets patrolling the skies over the city. My fellow analyst Maurene Caplan-Grey reports that military radar around New York City is interfering with television reception. Both of these disruptions, the sounds of jets and radar interference, are minor inconveniences, reminders to those of us not devastated, hurt, killed, widowed or orphaned by the 11 September 2001 attacks that peace has ended. Continued on page 2

Gartner

The tectonic events that began with the attacks of 11 September on New York City and Washington, D.C., have not ended, and our lives and businesses will be very much affected by the "war on terrorism." A friend of mine who was in the Pentagon that day said: "This feels like defeat — it was a defeat. The terrorists have won the first battle." And there are many battles to come.

Military strategists writing on what is called "the fourth generation of warfare" (4WG) discuss the blurring of the boundaries between peace and war. In 4WG, there is no differentiation of civilian and military targets; prime corporate property is a target for terrorists, and, therefore, business operations require greater distribution of critical assets, especially people. But distributing people relies upon collaborative systems — systems that are notoriously difficult to secure. Hence, new ways of doing business will open up new vulnerabilities.

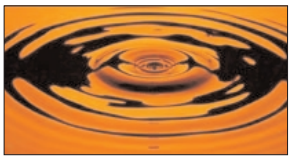
In this special Gartner Spotlight, Dan Miklovic and his team offer precise advice that clears the fog over a business environment that will be shaped by a prolonged war on terrorism (see "The Aftershock: A New Business Reality," AV-14-5685). Invariably, in calling for a wartime mobilization of business, we will be accused of overstepping our role. Ultimately, it is the business leadership's conscious decision about the context in which they want to consider our arguments and analysis, but I offer this pre-emptive response: In this new kind of war, business readiness and resilience are your most effective deterrents to terrorism. We are not going to return to business as usual, but we can get back to business.

Finally, I offer the reminder that business survival means more than just digging in — it means growing revenue and growing markets. This war on terrorism will challenge business not just financially, but also ethically. IT-related issues of privacy, financial secrecy, export controls and encryption are all squarely back on the public policy table. To wage a war against terrorism where the important victories will depend more on diplomatic, intelligence and social strategies than on military action, new regimes for technology-related regulatory issues are needed. Ethical behavior and corporate responsibility will be essential to their effectiveness and to victory over terrorism.

French Caldwell
Editor in Chief
Business and Public Policy

Article Overview

The Aftershock: A New Business Reality



The scope and nature of the "war on terrorism" remain unclear. Its effects on the business climate will differ from those of previous wars, and enterprises have forgotten much of what they knew about mobilization.

People worldwide wonder what the "war on terrorism" declared by global leaders really means, besides more uncertainty all around. Its effects have started to appear in odd ways. For example, residents living 50 miles northeast of New York City report severe interference with the city's television channels broadcast via cable TV.

The cable provider cited the government's increased use of radar as the cause. Likewise, the "war" will likely affect the business climate in unexpected ways. Since this war will not be like previous wars, such as World War II and the Vietnam War, the war economy will probably not resemble past war economies.

Still, the mobilization efforts will affect business substantially. Enterprises will feel some impacts immediately and directly, such as by the loss of key workers activated as military reservists or National Guard members. Other effects will be more indirect, such as a return to "lumpy" supply and demand wrought by the supply chain disruptions and shortages of materials that a war effort might spawn. Smart enterprises in both the public and private sectors will try to assess the impacts of this uncertain, evolving economy and make adjustments in operations, strategies and even business relationships.

Businesses can prepare for the war economy, and many of those that do can emerge as the next generation of "blue chip" enterprises. "How to Prepare for the Campaign Against Terrorism" (TG-14-5440) provides an overview of a wartime economy, something beyond the institutional memory of many enterprises — even before the existence of some. "War Will Change the Business Environment" (TG-14-5398) addresses the impact on operations and business relations, which will place new demands on business applications. "Using the Internet to Distribute Operations in Wartime" (TG-14-5419) describes how enterprises should plan to restructure to reduce vulnerabilities.

Enterprises will also need to pay attention to specific areas that are crucial for the enterprise to remain viable. "Safeguarding the Workforce in Uncertain Times" (COM-14-5682) delves into the effect on human capital. Enterprises will of course have to ensure that their networks remain secure from physical and cyber assaults — see "Quiz Your Service Provider About Security" (TG-14-5503). In addition, the heightened awareness of terrorism will lead government to change the rules in many areas, such as privacy, and telecommunication companies and their customers will have to wrestle things into a new order — see "Telecom Challenges in the Face of Global Terror" (TG-14-5684). The changes wrought by the events of 11 September will have a truly global reach. Lest anyone believe that the war on terrorism will affect the United States predominantly, "The War on Terrorism Will Affect Euro Conversion" (TG-14-5618) explains that the fallout has already affected the euro conversion process.

Elements of business operation and management will also feel the effects early on. "Protect Your Infrastructure in Wartime" (DF-14-5485) offers advice that will prove to be beyond the experience of many enterprises. Even strategic planning takes on a new importance but becomes more burdensome as well — see "Strategic Enterprise Planning in Wartime: A Battle in Itself" (TG-14-5479). Enterprises will increase their reliance on certain applications, such as supply chain management, in the face of the logistics and inventory realities of this new war — see "Planning for Wartime Effects on the Supply Chain" (COM-14-5525). In addition, some manufacturing technologies hold lessons for IT generally on how to cope with disruptions — see "Industrial Control Can Instruct Robust IS Practices" (TU-14-5619). Finally, emerging technologies that many enterprises hesitated to adopt will move more quickly into the mainstream. "Emerging Technologies to Minimize Disruptions: Checklist" (T-14-5578) explains what they are and how they could differentiate competitive enterprises from marginal performers.

Feature/Summaries

How to Prepare for the Campaign Against Terrorism

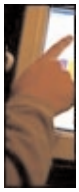
by French Caldwell, Charles Abrams and Kristian Steenstrup - 19 September 2001

Industry, especially the IT sector, will need to reallocate resources to a long, sustained campaign against global terrorism. Enterprises should make plans in five areas.

Protect Your Infrastructure in Wartime

by William Malik - 24 September 2001

Wartime leaves enterprises vulnerable to disruptions in critical infrastructure. Enterprises should immediately assess their risks in personnel, supplies, finances and technology, and develop contingency plans.



Using the Internet to Distribute Operations in Wartime

by Kristian Steenstrup, John Girard and Dan Miklovic - 21 September 2001

The Internet and the distributed computing model are more than just IT architectures — they offer a metaphor for how enterprises can reduce their vulnerability to wartime disruptions.

Telecom Challenges in the Face of Global Terror

by Marcus Breen - 25 September 2001

Defense and security concerns will postpone plans to make additional spectrum available for 3G wireless. The "war on terrorism" will call on the telecom industry to help. Carriers and enterprises can help formulate policies and regulations.

Quiz Your Service Provider About Security

by John Pescatore - 21 September 2001

The war on terrorism will only increase the risk of "cyberattacks," and enterprises that use service providers depend on their diligence. Make sure yours has implemented solid security services and controls.

The War on Terrorism Will Affect Euro Conversion

by Andrea Di Maio and Nick Jones - 25 September 2001

Euro program managers must revise their plans for the final euro changeover steps because of the disruptions caused by the recent terrorist attacks.

Feature/Summaries

Planning for Wartime Effects on the Supply Chain

by Jeff Woods and Karen Peterson - 24 September 2001

The campaign against terrorism will affect business operations and supply chain projects. Enterprises should know the four areas where the pain will be felt and what tools to evaluate in response.

Safeguarding the Workforce in Uncertain Times

by Diane Tunick Morello, Bill Keller, Jenni Lehman, Michael Bell and Cassio Dreyfuss - 25 September 2001

Through smart handling of people, knowledge and work settings, enterprises worldwide can prepare for an uncertain global business climate. They should take steps in six areas.

War Will Change the Business Environment

by Dan Miklovic, Kenneth Brant, Brian Zrimsek, Andy Kyte - 24 September 2001

As an entirely new type of war evolves, business operations, applications and relationships must change. Flexibility will be more important than ever, but the new environment has other implications as well.

Emerging Technologies to Minimize Disruptions: Checklist

by Kathy Harris and Jackie Fenn - 26 September 2001

The "war on terrorism" could potentially become the most-disruptive force enterprises must face during the next 10 years. The emerging technology sector will shift its focus to address this challenge.

Industrial Control Can Instruct Robust IS Practices

by Kenneth Brant and Dan Miklovic - 24 September 2001

Distributed control and system reliability have matured in mission-critical industrial environments. These concepts can instruct IS practitioners on the design and maintenance of robust business systems as risks of disruption increase.

Strategic Enterprise Planning in Wartime: A Battle in Itself

by Andy Kyte - 26 September 2001

Although enterprises must focus on how the war on terrorism will affect operations, they will need to devote extra effort and resources to strategic planning.

Aftermath: Disaster Recovery and Business Continuity

Letter from the Editor

21 September 2001

Enterprises worldwide are struggling to come to terms with the sheer human impact of the recent terrorist attacks on the United States, and are trying to find ways to return, as they must, to normal business operations. Gartner is determined to assist their efforts in every way possible, and has prepared this special edition of our Security and Privacy Spotlight to help enterprise decision makers manage disaster recovery and business continuity planning (BCP).

Some enterprises have been able to leverage their year 2000 efforts—particularly BCP and year 2000 command centers—to respond to disaster threats. Most enterprises, however, developed plans merely to satisfy audit requirements, and suspended their contingency planning efforts shortly after 1 January 2000. As a result, their plans could not be applied to the 11 September 2001 disaster because enterprises, processes and personnel change over time, and plans must be tested to cover new conditions. Nonetheless, enterprises can frequently leverage the processes used in addressing the year 2000 crisis to respond to new disasters. For this reason, we have adapted some archival Gartner research on BCP for this issue.

We are confident that this special edition will prove valuable to enterprises in the coming weeks and months of recovery, and in the years of planning and preparing for disasters that are certain to follow.

Victor S. Wheatman
Editor in Chief
Security and Privacy

Article Overview

Aftermath: Disaster Recovery

Gartner estimates that two out of five enterprises that experience a disaster will go out of business in five years. Enterprises can improve those odds — but only if they take the necessary measures before and after the disaster.

The terrorist attacks on the United States on 11 September 2001 are focusing the attention of enterprise decision makers on the urgent need to prepare for disaster recovery — i.e., the steps an enterprise takes when it cannot operate normally because of a natural or manmade disaster. Before 11 September 2001, most enterprises may have thought of a disaster in terms of a snowstorm that hampers operations because key operating personnel cannot reach their positions. Recent events make it clear that the word “disaster” can mean something far more catastrophic — events from which it may take months or even years to recover. This special edition of the Security and Privacy Spotlight examines the issues of disaster recovery, business continuity planning (see “Aftermath: Business Continuity Planning,” AV-14-5138), and the tools and services required for both (see “Aftermath: Technology Tools and Services,” AV-14-5338).

The reality is that many enterprises that experience a disaster never recover. Gartner estimates that two out of five enterprises that experience a disaster go out of business within five years. In some cases, the disruption of normal business operations causes customers to lose confidence in the enterprise's viability. In other cases, the cost of recovery is simply too great. Sometimes the failure is caused by the loss of key personnel — a problem that is likely to be critical for many of the enterprises affected by the destruction of New York's World Trade Center. Some of the financial services providers located in that complex are believed to have lost one-third or more of their personnel, including many senior executives, and many of these enterprises may find it impossible to recover.

An enterprise may declare a disaster for a number of reasons, both routine and dramatic:

- Extreme weather conditions (e.g., Hurricane Floyd, which brought the eastern United States to a standstill in September 1999)
- Prolonged power or communications failure (e.g., the difficulties faced by enterprises and individuals in New York after the World Trade Center attack)
- Robbery or other criminal activity (e.g., the theft of credit card numbers from CDNOW and other e-commerce sites)
- Civil unrest (e.g., the disturbances at the World Trade Organization conference in Seattle in 2000 and the Group of Eight summit in Genoa in 2001)
- Terrorist acts

Recent Gartner Dataquest research on application downtime shows that an average of 40 percent of downtime is caused by application failures (e.g., performance issues or "bugs"), 40 percent by operator error, and approximately 20 percent by system or environmental failures. The majority of the failures in the "system or environmental" segment — 60 percent — is caused by hardware problems. Overall, less than 5 percent of application downtime is attributable to disasters.

The disaster recovery section of this special edition of Security Matters! examines the steps that enterprises must take to recover from a disaster. These steps are usually detailed in a business continuity plan — but many enterprises have never prepared such a plan. The research included in this section outlines management's primary responsibility — protecting the health and safety of personnel — and the actions to be taken to ensure that business resumes as soon as possible. Planning is critical to these efforts: Gartner research shows that enterprises that have prepared business continuity plans are significantly more likely to survive than those that have not.

The damage a disaster causes to an enterprise may not necessarily be physical, as the troubling increase in systems- and operations-disrupting "cyberattacks" shows. These activities are certain to increase in response to any reprisals, including military action, that the United States takes in response to the 11 September 2001 attacks, and enterprises must immediately take precautionary measures. Communications — the lifeline of modern business, indeed of modern society — often fail during disasters. Landline telephone service may be lost, wireless networks and data lines may be damaged, broadcast radio and television may be knocked off the air. The events of 11 September 2001 show, however, that other technologies

— including e-mail, two-way paging and instant messaging — can enable individuals and enterprises to communicate under even the most difficult circumstances.

This section discusses a number of other key disaster-related issues, including: the impact of a disaster even on enterprises far removed from the disaster site; the importance of software change management methodologies; the available data replication technologies; and the importance of government action in ensuring business recovery.

A common thread runs through these research pieces: the urgent need to prepare for disasters that can threaten the very existence of an enterprise. Gartner's research makes it clear that comprehensive, proactive action can significantly improve enterprises' chances of survival — particularly if they begin preparing now.

Feature/Summaries

What Is Crisis Management?

by Roberta Witty - 19 September 2001

Disasters and other events that stop normal business processes require that management take immediate action to ensure the health and safety of personnel, and the viability of the enterprise.

The Ripple Effect: Disaster's Indirect Impact

by Donna Scott and Bill Gassman - 20 September 2001

The events of 11 September 2001 show that disasters affect even enterprises far from the scene of the event. Enterprises must begin preparing for these ripple effects immediately.

Jump-Start the Business Continuity Plan: A Checklist

by Roberta Witty - 21 September 2001

The 11 September 2001 terrorist attacks are different in their human and enterprise operational impact from previous disasters. Enterprises must act to ensure their business continuity in the wake of these and possible future events.

Software Change Management: Disaster Recovery Lessons

by Vic Wheatman and Chris Morris - 19 September 2001

The failure of the Australian Stock Exchange in 1995 shows the potential cost of even a brief interruption in service, and demonstrates that software change management is critical to uninterrupted operation.

Cyberattacks: Prepare Your Enterprise Now

by Rich Mogull - 20 September 2001

A significant increase in cyberattacks is likely to follow the events of 11 September 2001. Enterprises must understand this threat and take action to limit their vulnerabilities.

Disaster Recovery: Weighing Data Replication Alternatives

by Donna Scott, Josh Krischer and Jon Rubin - 15 June 2001

Enterprises with short disaster recovery time objectives use data replication technologies. We provide a framework for understanding the myriad of available options.

Feature/Summaries

Getting Through: Using E-Mail and IM in a Disaster

by Joyce Graff, Maurene Grey and Robert Batchelder - 20 September 2001

Standard communications methods can fail during natural and manmade events. However, as recent events have shown, alternatives such as e-mail, two-way paging and instant messaging may help get your messages through.

Disaster Recovery: What Governments Should Do Now

by Gregg Kreizman, Christopher Baum and Bill Keller - 20 September 2001

In the period following the terrorist attacks of 11 September 2001, governmental bodies at all levels must reassert themselves and take all necessary steps to ensure the continuity of government services.

Disaster Management Plan for Remote Access

by John Girard - 20 September 2001

Telecommuting and mobile access can help enterprises cope with emergencies. When disaster strikes, key company locations may go offline or be physically inaccessible. Remote work capability will keep businesses running.

Article Overview

Aftermath: Business Continuity Planning

In the past 10 years, BCP has broadened its scope from disaster recovery to business recovery. The 11 September 2001 attacks on the United States dramatically emphasizes and heightens BCP's necessity and importance.

History: 1990 – 2000

In the past 10 years, business continuity planning (BCP) has evolved into a major concern for corporate and IT decision makers, and the Internet and evolution of e-business have significantly increased its importance. The events of 11 September 2001, and the heightened awareness of enterprise vulnerabilities that will inevitably follow, present business continuity planners with enormous challenges — but also with an extraordinary opportunity to implement mission-critical changes. This special edition of our Security and Privacy Spotlight examines the issues of BCP, disaster recovery (see "Aftermath: Disaster Recovery," AV-14-5238), and the tools and services required for both (see "Aftermath: Technology Tools and Services," AV-14-5338).

In the early 1990s, business continuity was positioned mainly in terms of disaster recovery. In the event of a major disaster, technology assets (e.g., systems, networks, applications and data) were to be "recovered" in an alternate location. The typical recovery time objective (RTO) — i.e., the desired time to recover applications — was approximately three days; the typical recovery point objective (RPO) — i.e., the acceptable transaction loss — was 24 hours. Most of the enterprises that implemented disaster recovery plans did so because they were in highly regulated industries (e.g., banking and other financial services sectors). In most enterprises, however, business continuity and disaster recovery planners spent their time trying to raise awareness of the need to protect enterprise assets — often unsuccessfully — and fighting apathy toward recovery planning.

By the mid-1990s, business continuity initiatives had expanded to include the recovery of critical work processes. For example, many enterprises recognized that recovering their call center technology was pointless if they lacked personnel to staff the call center itself, or a workplace in which to locate it. BCP and disaster recovery scenarios remained largely unchanged, however, as did RTOs and RPOs.

The trend toward an expansion of BCP initiatives gathered momentum in the late 1990s, driven in part by preparations for potential year 2000 crises. One result of year 2000 remediation was massive enterprise investment in re-engineering business processes (e.g., implementing integrated enterprise resource planning systems). As they prepared their year 2000 contingency plans, many enterprises began to understand that if their critical systems and applications failed, their business processes would fail along with them — e.g., orders could not be taken and products could not be manufactured or shipped. The inevitable result would be a severe negative impact on the profitability and possibly the survival of the enterprise. Due to this new understanding of their vulnerabilities, enterprises invested heavily in BCP and disaster recovery between 1997 and 2000. RTOs for mission-critical business processes were reduced to less than 24 hours and sometimes much less; RPOs were often set as up to the point of disaster — i.e., no loss of work or transactions. Moreover, the growing interdependencies among internal processing systems and external service providers began to increase the complexity of recovery solutions. Nonetheless, scenario planning remained largely unchanged.

The Internet Changes Everything

The arrival of the Internet and e-business — which achieved critical mass in 1999 — caused fundamental changes in the way enterprises thought about BCP. Enterprises began re-engineering their business processes yet again, this time integrating them with those of customers, suppliers and business partners. As a result, RTOs and RPOs have been reduced still further, in some cases reaching zero. (A zero RTO means zero downtime, or 24x7 continuous business process availability.) Furthermore, scenario plans have broadened to take on new e-business-specific risks, including downtime caused by:

- Operational risk (e.g., the three-day Microsoft Web site outage in January 2001)
- Security risk (e.g., denial-of-service attacks against Web sites and networks)
- Lack of capacity (e.g., the spikes in business volumes caused by Victoria's Secret's Internet fashion show)

- Application failure (e.g., the full-day London Stock Exchange outage in April 2000)
- Partner/outsourcer unavailability (e.g., Internet service provider network failure or failed links between an enterprise's Web site and its partners' sites)
- Loss of physical structures (e.g., facilities lost to wildfires at the Los Alamos National Laboratory)

In the new e-business world, enterprises must be deeply concerned about any risk of downtime. Today, any downtime results in negative media coverage, which can severely impact the enterprise's image and reputation — and its continuing viability.

BCP Today: Enterprise Survival Depends on It

In a way, the terrorists attacks on 11 September 2001 complete this 10-year evolution in BCP — but they also change everything. The dramatically heightened recognition of the importance of business continuity means increased budgets for dedicated, nonshared recovery solutions for business applications and systems of all types. Planners will have the opportunity to integrate business continuity into the project life cycles of business processes and applications. Old and new risks can be addressed where they should be — in the business requirements phase of a project, not as an afterthought when production has been completed. Most important, there will be newfound business continuity planners. After 11 September 2001, enterprise decision makers understand why business continuity is important: The survival of the enterprise depends on it.

The task of implementing comprehensive BCP will certainly be easier now, in part because enterprises in general are much more organized for business continuity today than they were before 2000. Due to the growth of e-business, and now the heightened appreciation of BCP, by 2005, more than 70 percent of large enterprises will have invested in BCP, compared to fewer than 25 percent today (0.8 probability).

The BCP section of this special edition of Security Matters! further examines these issues and, particularly, the impact of e-business on BCP initiatives. The research in this section points to a fundamental truth: E-business is blurring the lines between those who are insiders to our business and those who are outsiders. It is also blurring the lines between the production environment and the recovery environment. They are now one in the same, and recovery requires collaborative continuity planning among all interdependent parties. This has been true for several years. The events of 11 September 2001 brings this truth, tragically, into sharper focus.

Feature/Summaries

Business Continuity Planning and Management: Perspective

by Kristen Noakes-Fry and Trude Diamond - 12 September 2001

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.

Integrating BCP Into the IT Project Life Cycle

by Roberta Witty - 15 June 2001

To maintain customer confidence and financial stability in the event of a disaster, BCP must be addressed at the beginning of an IT project. Here, Gartner describes how BCP can be integrated into the IT project life cycle.

Enlightening the CEO on Business Continuity Planning

by Donna Scott - 30 June 1999

Many business continuity and disaster recovery planners complain they cannot get visibility in the boardroom. We offer advice on gaining visibility and the commitment required for effective continuity planning.

Fault-Tolerant Networks: Is There Such a Thing?

by David Neil and Bob Hafner - 14 June 2001

When ensuring business continuity, often only cursory attention is paid to the robustness of the communications network. We offer guidelines and considerations to improve the resilience of an enterprise's communications facilities.

How E-Business Is Changing Business Continuity Programs

by Fred Luevano - 14 June 2001

Our executive interviews at the March 2001 Disaster Recovery Journal Conference confirm the trends in how e-business is impacting business continuity and disaster recovery programs.

Article Overview

Aftermath: Technology Tools and Services

Disaster recovery and business continuity planning are complex and highly specialized fields. Enterprises need detailed information to help them make mission-critical decisions about these technologies and services.

Business managers — not just IT managers — know that little of value is accomplished without planning. Planning for disruptions and discontinuity in business operations is particularly difficult. Disasters — large and small, natural and manmade — are by their very nature infrequent and unforeseeable events. Perhaps the key inhibitor to planning in this area, however, is denial — i.e., "It can't happen here." The 11 September 2001 terrorist attacks on the United States make it painfully clear, however, that "it" can happen anywhere, and enterprises must plan for disasters and their consequences. This section of our special Aftermath Spotlight examines the technology tools and services required for business continuity planning (BCP — see "Aftermath: Business Continuity Planning," AV-14-5138) and disaster recovery (see "Aftermath: Disaster Recovery," AV-14-5238) decisions. As recent events make all too clear, these decisions are and will continue to be critical to the survival of many enterprises.

When to Implement a BCP Software Application

Disaster recovery and business continuity planning (BCP) ensure that tactical procedures are in place to meet every type of challenge that can be realistically anticipated. Precautionary measures are frequently mandated by government regulation, industry policies or auditing requirements — but they are also simply good sense. Whether an enterprise should implement a BCP software application to assist with the task depends on a number of factors, including:

- Whether a business continuity plan is already in place
- Available in-house resources
- The degree of control local managers retain over business continuity

How can an enterprise assess these factors objectively and match its requirements to available solutions — high- and low-tech? Which solution justifies the sustained, enterprisewide commitment that BCP requires?

The tools and services section of this special edition of the Security and Privacy Spotlight gives detailed guidance for enterprises struggling to answer these mission-critical questions about disaster recovery and BCP technologies, services and vendors. We discuss the process of selecting technology vendors and service providers, and the fine points of contract negotiations in this highly specialized market, which is dominated by a small number of providers, with a few, smaller vendors handling special needs or specific platforms — this is of significant concern. One of the leading BCP providers is facing bankruptcy, and others are repositioning their offerings; therefore, we provide an overview to help in vendor selection. We also examine tools that can help decision makers assess enterprise risk and determine the potential effectiveness of prescribed safeguards. Finally, we offer profiles of several important disaster recovery solution vendors.

Feature/Summaries

Building an RFP for Business Continuity Services

by Simon Mingay - 27 August 1999

We outline what needs to go into an RFP when assessing potential providers of BC and disaster recovery services.

Negotiating a Sound Business Continuity Contract

by Simon Mingay, Donna Scott and Roberta Witty - 21 September 2001

Enterprises negotiating business continuity services contracts must consider a number of key issues that can mean the difference between a good deal and a bad one.

Business Continuity Moves From Management to Access

by Tony Adams - 21 August 2001

IT services, including disaster recovery and business continuity planning and management, has long been the focus of a specific breed of service offerings. Focused on protecting businesses from the consequences of unexpected downtime, these traditional offerings are likely to be joined in the marketplace by newer value propositions, which are more in the line of sight of corporate officers and line of business managers. Gartner Dataquest examines the moves made by this sector of the service industry to reinvent itself.

SunGard Business Continuity Services

by Kristen Noakes-Fry and Trude Diamond - 20 September 2001

SunGard Recovery Services has added new hosted disaster recovery facilities and mobile data centers, as well as new features. New "eSourcing" Internet business continuity services further expand the options beyond the recovery site. As disaster recovery services expanded into full business continuity planning and management (BCPM), encompassing everything from continuity planning to large, private communications networks, SunGard definitely got in on the ground floor. From its roots in disaster recovery, SunGard has developed continuity planning software products— PreCovery and ePlanner software— to manage the overwhelming detail of BCPM projects.

Sourcing Recovery and Continuity Services

by Simon Mingay - 12 June 2001

The decision on whether to outsource recovery and continuity services is becoming more complex. Here we consider the factors influencing such a decision and the approaches enterprises are taking.

Feature/Summaries

IBM Business Continuity and Recovery Services

by Kristen Noakes-Fry and Trude Diamond - 21 September 2001

IBM's continuity services help organizations maintain critical business continuity and recovery functions in an emergency through customized continuous availability, rapid recovery, and hot-site recovery. While IBM is by no means the only disaster recovery service provider in the industry, over the past 11 years IBM Business Continuity and Recovery Services has grown to become the biggest. Acts of terrorism, unpredictable natural disasters, infrastructure failures, or unexpected downtime with hardware or software cost individual companies thousands of dollars in lost equipment and company productivity. Downtime—even minutes for a high-availability system—can represent a serious business interruption. With these services, IBM enables business continuity and Internet security management on the enterprise level.

BCP Tools: Your 'Friend in Business'

by Kristen Noakes-Fry and Ant Allen - 15 June 2001

Creating a business continuity plan demands skill, expertise and experience that those responsible for an enterprise's BCP may lack. A software-based planning tool may be used as part of the solution.

Comdisco Business Continuity and Recovery Solutions

by Jennifer Gordon - 22 February 2000

Comdisco Continuity Services, part of Comdisco, Inc., is one of the leaders in the business continuity (BC) arena, maintaining the most experience and arguably the most comprehensive offering of recovery services in the U.S. BC industry. Comdisco provides a range of global technology management services to meet the needs of mainframe, distributed, and work-area computing worldwide. The company has over 20 years of business continuity and recovery experience under its belt and has a high visibility in the U.S. With more than 100 locations around the world, Comdisco serves more than 4,000 customers in North and South America, Europe, the Pacific Rim, and Australia. It is also one of the leading providers of continuity services in the United Kingdom and France and continues to improve its pan-European offerings.

Gartner