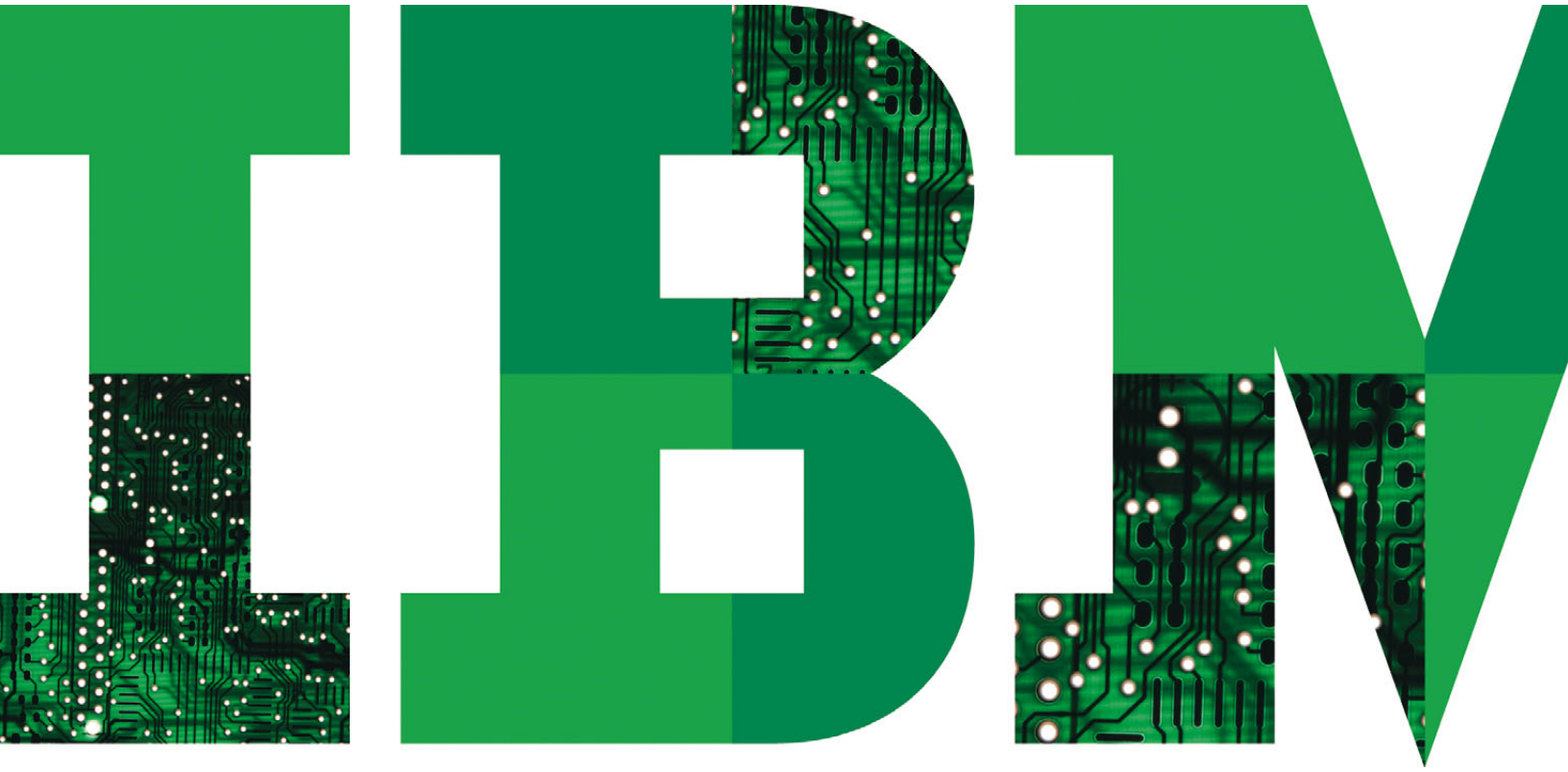
IBM Global Technology Services
Thought Leadership White Paper

May 2011

Proactive technical support: The overlooked essential in business resilience

Combine hardware and software technical support with business continuity and disaster recovery plans



IBM

Contents

Introduction

Today's business environments are at their most complex. Enterprises continue to undergo rapid change while facing the heightened impact of business disruptions and coping with a volatile financial and regulatory landscape. The possibility for business disruptions has increased exponentially, and so have the ramifications. Yet when planning for business continuity, many organizations overlook the importance of technical support. Hardware and software failures are often perceived as routine occurrences, but without a proactive management approach, they can quickly evolve into full-blown disasters with significant financial and reputational consequences. For this reason, successful organizations reinforce their business resilience strategy with proactive hardware and software technical support. As shown in responses to the 2010 IBM Global IT Risk Study, many others still do not.

In fact, in light of the risks associated with business disruptions in today's climate, responses to the IBM Global IT Risk Study—a comprehensive online survey of 556 IT managers and others primarily involved in their business's IT functions—uncovered a surprising paradox. Fifty-four percent of respondents said their overall approach to mitigating IT risk was good. However, only 23 percent of respondents believed their organizations were well prepared for hardware and software system failures. And when asked to list the kinds of risk issues they had dealt with in the previous 12 months, respondents ranked systems failures second only to security breaches.[1]

As the respondents' experiences would indicate, hardware and software support are critical to an effective business resilience strategy. Yet organizations often spend their time focusing on other, albeit equally important, elements of business continuity, including a range of provisions to avert interruptions—from normal business events to unforeseen catastrophes. These provisions include backup servers, data mirroring, data backups, offsite data storage and disaster recovery. While all of these elements are critical, they can fall short of meeting daily needs for system availability. Without hardware and software viability, organizations are only as strong as their weakest link.

For example, one of the basic tenets of business resilience is maintaining data and service availability, both of which are directly threatened when software and hardware failures occur. Unplanned outages can create far-reaching consequences that impact long-term revenue streams, brand reputation and survival. The potential impact may be more prevalent than previously thought. In fact, a March 2011 report on UK businesses revealed that more than 80 percent of business interruptions in 2010 were due to hardware failures. The report also revealed that more than 50 percent of hardware failures were a result of inadequate maintenance in place to protect equipment against failures.[2]

Software errors can be equally damaging. In late 2009, a major online reseller saw its site crash, just in time for holiday shopping, due to a software error that collided with a surge in web site traffic.[3] In January 2009, Google's search engine erroneously notified users that every web site worldwide was potentially malicious, including its own. A programmer's misplaced forward slash (/) was to blame.[4] In another case, a software problem contributed to a rail car fire in a major underground metro system in 2007 when software designed to monitor performance did not detect overheating.[5] The 2003 North America blackout was triggered by a local outage that went undetected due to a flaw in the monitoring software.[6]

Even with these numerous occurrences, effective hardware and software support—while often addressed within the organization—are often not included as part of a comprehensive business resiliency plan; in many cases business continuity is managed in one silo, and hardware and software support in another, hindering cross-infrastructure visibility and leaving the business exposed to risk.

Organizations must be able to answer questions like:

What would happen if a Microsoft Exchange server on which corporate emails are stored were to crash? Are there provisions for server technical support and maintenance, in addition to backup servers?

How long, if at all, would business operations continue if an email server became unavailable?

What are the provisions for releasing fixes and updates for microcode and business-critical applications, and for ensuring that these are applied at every endpoint where the applications are in use? Security patches can require distribution in near real time. Is the organization prepared to do so?

What is the plan to prevent servers that house customer-facing web services from crashing?

This white paper will discuss the foundational elements of a strong business resilience plan, which must holistically include not only the generally established capabilities for business continuity and disaster recovery but also hardware and software support.

In a recent survey of 200 disaster recovery decision makers and influencers conducted jointly by Forrester and the Disaster Recovery Journal (see Figure 1), when asked, "What was the cause(s) of your most recent disaster declaration(s) or major business disruption?", twenty-four percent of respondents cited IT hardware failure, second only behind power failure. Eleven percent of respondents cited software failure as the culprit.[7]

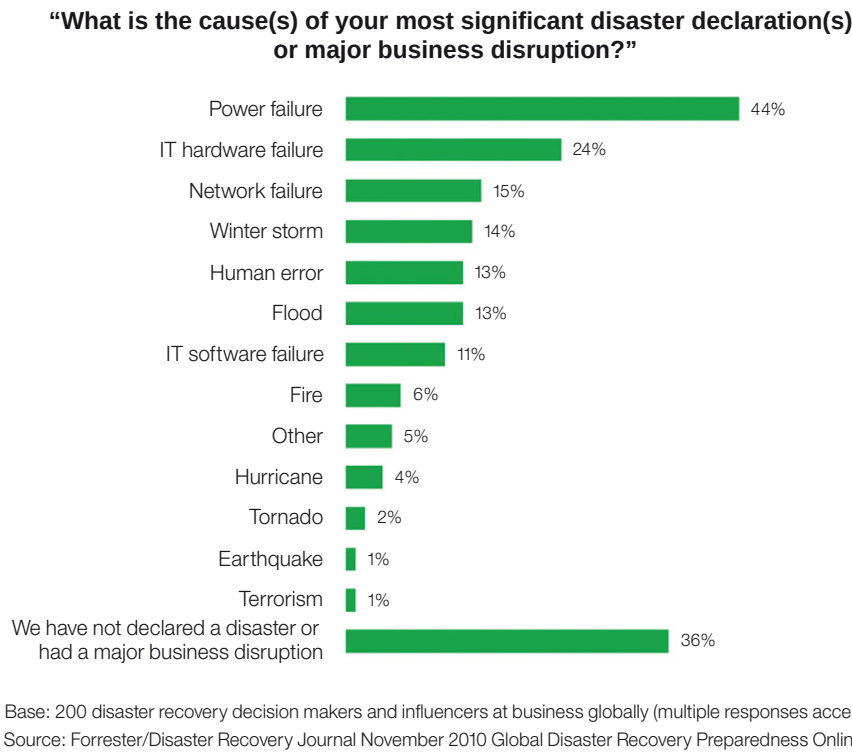


Figure 1: A 2010 Forrester/Disaster Recovery Journal survey revealed hardware failures were ranked second only to power failures as the most common source of a recent disaster or business disruption.

Addressing risk driven by business, events and data

A comprehensive, successful business resilience strategy includes provisions for ensuring continuous business operations and around-the-clock global service delivery, providing the ability to act with speed and agility when an unforeseen event strikes. To accomplish this, organizations must address all potential challenges to business resilience, which can be divided into three categories: business-, event- and data-driven events.

Most business resilience strategies address business-driven events, such as audits, new product rollouts, future marketing promotions, or failure to meet industry standards. They also address event-driven risks, such as natural disasters, regional power outages, acts of war or economic downturns. In fact, organizations today may be the best prepared to manage the latter, understanding the need to quickly react to revenue shortfalls and drastic shifts in business goals.

The missing piece for many business resilience strategies is in effectively and proactively addressing the possibility of data-driven events, such as data corruption, disk failure, application outages and network problems—which can sometimes be traced to software or hardware system failures. The reality is that if organizations have a strong business continuity program that includes network, application and data security but inadequate levels of technical support, they are putting the business at risk on a day-to-day basis. An operating system without the latest patches and fixes installed can spread a virus to backup servers, for example. Likewise, an older version of microcode on a server can cause failures when new applications are installed.

Indian bank speeds time to market by combining disaster recovery with IT infrastructure maintenance

A regional bank in India wanted to provide "anywhere banking" services to customers to secure competitive advantage, yet its small IT team was unable to manage the undertaking alone. The bank engaged IBM to build a comprehensive business resilience plan that combined disaster recovery—including procedure documentation and drill support—and IT infrastructure maintenance, including 24×7 comprehensive monitoring and management services for servers, storage, networks, security, backup and databases. The combined disaster recovery and infrastructure maintenance strategy reduced the bank's upfront capital expenditure for web-facing systems. It also eliminated the need for multivendor coordination, enabling the bank to better use existing IT staff and ultimately increase time to market for new service delivery. Total cost of ownership went down while ROI increased.

Redefining the requisite elements of business resilience

Most business resilience plans have mainly focused on business continuity and disaster recovery, including provisions for backup servers, data mirroring and failover to protect data after failures occur, but in order to prevent failures, organizations must take a more holistic approach by incorporating hardware and software maintenance and support into the overall business resilience plan. Both prevention and remediation are critical, yet often the two are addressed by separate IT teams. This makes it difficult to provide a cohesive approach to business resilience that can cover enterprise and work area risk, IT stability, recoverability of the IT infrastructure, data backup and disaster recovery—as well as availability of critical data and business applications. It is these last two, data and application availability, that require a comprehensive hardware and software support strategy that can meet the demands of enterprises facing rapid change and a volatile, highly regulated marketplace—a marketplace that depends on the secure and continuous flow of information. Uninterrupted business operations, and even ongoing business strategy, hinge on the ability of hardware and software to enable the transformation of data into that information. Addressed separately, technology, software and hardware, and even the data they contain, become useless. Integrating the layers of business resilience, and addressing hardware and software support within those layers (see Figure 2), is essential.

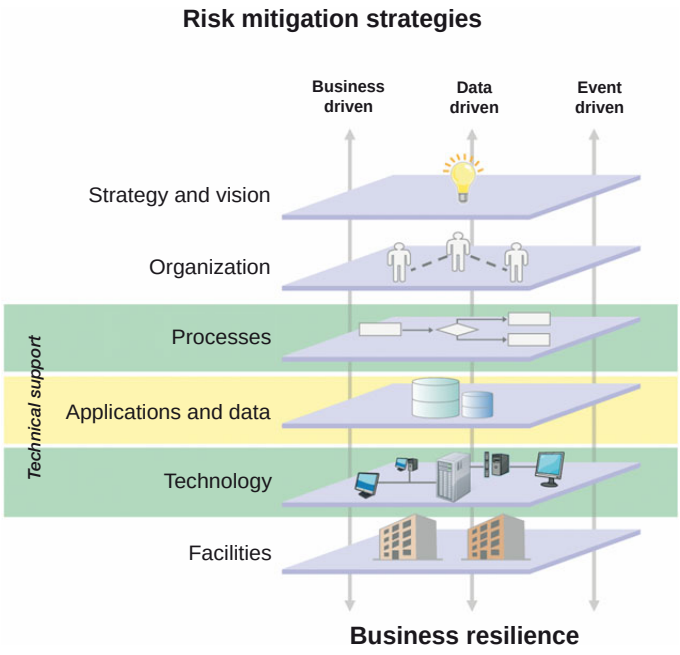


Figure 2: To maintain the continuous flow of information required to support uninterrupted business operations, each layer shown above must be integrated within a comprehensive business resilience framework that provides for business-, event- and data-driven events. Hardware and software support should be addressed within the technology, applications and data, and processes layers.

Freight railroad increases efficiency and flexibility with new business resilience plan

A North American freight railroad that services 23 states and two Canadian provinces relies heavily on 24×7 application availability but lacked a disaster recovery facility. The company worked with IBM to establish data mirroring capabilities that would help them achieve near real-time recovery point objectives, as well as hardware and software maintenance and support across multiple vendors. Afterward, the railroad incorporated all its equipment and applications, from IBM and other vendors, into a comprehensive business resilience plan. The transition was so seamless that customers and supply chain partners requested that additional applications be included in the plan. By adding new technologies like virtualization into their data center, the railroad established data center portability, self-healing and greater flexibility during business recovery.

Foundational business continuity for today's infrastructures

Best-in-class companies take a holistic approach that combines planning, prevention and remediation to help solidify ongoing business operations. Yet this may be easier to accomplish in theory than in practice. The challenge is that today's data center is a mixture of vendor products and platforms, and is more difficult to support in a coherent way. Faced with staffing and budget limitations, few organizations can maintain a stable of experts on every platform and product on which they do business. This adds complexity to maintaining not only data availability, but also security and consistent resilience policy enforcement.

With this in mind, a comprehensive business resilience strategy built for the needs of today's IT infrastructures should include:

- A tested and proven business resilience program and plan that addresses business continuity, disaster recovery and hardware and software support
- Support for regulatory compliance and governance requirements
- Consistent policy enforcement across departments, corporate divisions and global locations
- Offsite data center and work area recovery capabilities, including alternate employee workspaces
- A tested and proven data backup and archiving system with offsite storage
- Appropriate system redundancy, ranging from onsite backup servers and storage to offsite mirrored systems with automatic failover
- Security, privacy and data protection to guard against internal threats (such as data theft) and external threats (such as viruses)
- Technical processes, including change management and application testing, that help prevent system failures
- Hardware maintenance and support for multivendor environments
- Software maintenance and support that provides fast access to deeply skilled expertise
- Remote support capabilities (including execution of fixes and patches) and web self-service to provide access to technical expertise, help prevent failures and speed problem determination and resolution.

IBM's Modular Support Services Are Designed to Optimize Your Support Today and Tomorrow

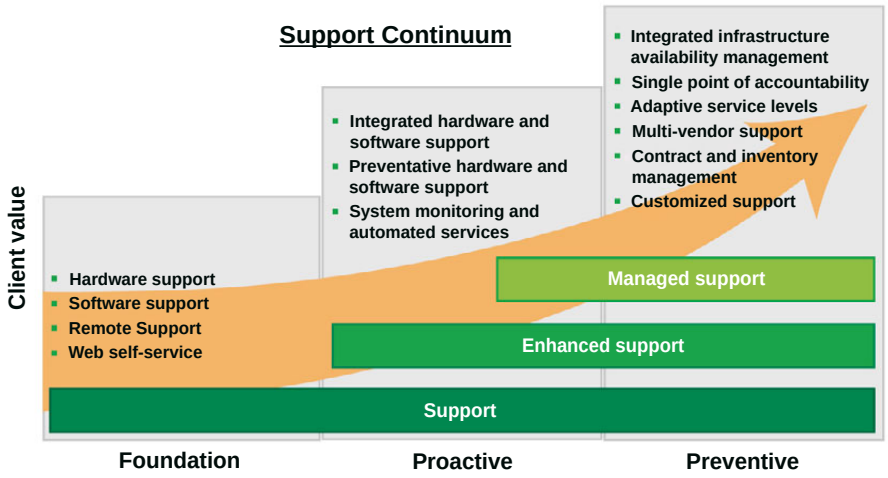


Figure 3: Hardware and software support is a foundational component of business resilience. Organizations can further enhance business continuity by adding capabilities such as system monitoring and integrated infrastructure availability management.

IT services provider leverages single contact for disaster recovery

A company that provides a passenger service system and data center services for one of the largest airlines in Indonesia had a local backup system in place but no disaster recovery solution, which the company needed to implement prior to their initial public offering. The company engaged IBM to create a comprehensive disaster recovery solution with ongoing disaster recovery support, including a data center and disaster recovery center facility, 24×7 managed services, and mainframe maintenance. Today, the company has a single point of contact for hardware and a majority of its software and operating systems, services and communications; a comprehensive disaster recovery solution; and a secure environment for its IT equipment.

Japanese business achieves one-day disaster recovery and critical hardware support

Previously, the largest publication distributor in Japan managed the recovery of its bookstores' operating systems and applications in-house—a time-consuming, resource-intensive process. The company needed to accelerate the recovery of mission-critical files and applications during frequent unplanned outages. Today, IBM provides file recovery support and disaster recovery services for the company's applications, operating systems and hardware within one business day. IBM also provides ongoing maintenance and software troubleshooting services. The company has improved service levels, and outsourcing enables the distributor's IT team to focus on core competencies while reducing recovery costs.

Beyond foundational resiliency: transferring risk

No matter the approach to developing a business resilience strategy, every organization must first understand its risks and then take action to mitigate those risks. For risk mitigation, it is sometimes more cost-effective and strategic to transfer the risk to a skilled vendor rather than invest in the skills training and capital outlays that may be required to maintain consistent and high-functioning business operations in the face of a business-, event- or data-driven event. In this case, managed support (see Figure 3) can help organizations achieve enhanced IT availability to support the continuous availability of business operations.

Organizations seeking advanced capabilities for business continuity and disaster recovery may require:

Event-driven managed services to meet recovery time and recovery point objectives after a business disruption, including fast backups, restores and critical data archiving, to help mitigate business impact. Other capabilities that may be required include workload balancing, limiting data loss via email recovery and supporting workforce resiliency through emergency notifications.

Outsourced recovery of IT and business infrastructures, including work areas, from disruptions to help reduce costs and timeframes related to lost employee productivity. Capabilities for maintaining continuity of critical systems, protecting against loss of key business data and employee productivity, and meeting regulatory compliance mandates can help prevent business disruptions.

Security-rich, automated protection of critical business data through onsite and offsite cloud-based services to reduce the need for infrastructure build-out to protect and store massive amounts of data.

Auditable compliance with general and industry-specific regulatory requirements to help track data access and prove data protection to avoid violations. Unproven security policies and procedures for widely distributed data can open the door to public disclosure requirements.

Holistic support focused on application availability for the end user rather than isolated server and storage availability. A view into how hardware availability affects software availability, which, in turn, greatly impacts business continuity, is critical.

Deep technology expertise, including an understanding of the inter-relation between applications and infrastructure components, especially in complex environments such as virtualization. Today, services and resources are distributed across what had been isolated domains—which means older management tools may be ineffective. Deep expertise and insight can prevent hardware and software failures from impacting business-critical services.

Integrated hardware and software capabilities, including cross-platform and multivendor technical support and proactive microcode and release management, which can help prevent failures and remove complexity. As new solutions are added to the infrastructure, they create additional points of failure. Proper change orchestration across hardware and software updates and maintenance is crucial.

A single point of accountability across vendors based on consistently agreed upon and continuously monitored service levels, which can significantly improve availability management and speed time to resolution by avoiding finger pointing during problem isolation.

Proactive monitoring to minimize or eliminate the business impact of technical problems by continually tracking the health of the IT infrastructure via real-time dashboards, which can help anticipate future problems and notify IT to take preventive action.

Contract and inventory management capabilities, which are essential to maintaining compliance and controlling IT asset costs. License compliance and inventories can be tracked automatically, removing manual, inaccurate oversight while avoiding over-purchasing and under-licensing.

Customized support, which is especially relevant for multivendor, multidomain environments where complex dependencies can wreak havoc on administrators who do not have the insight or time to manage this type of infrastructure.

Data storage company transfers risk to improve service delivery

A data storage company that provides hardware devices and data management software to customers in virtually every industry had previously provided ongoing product support via internal resources and a network of seven individual third-party maintainers (TPMs) in the United States and dozens of TPMs worldwide. Product support was poor, and the business suffered. The company integrated its customer relationship management system with IBM's, allowing IBM service representatives and engineers to respond to technical support calls and requests for on-site support. Providing customers with a single point-of-contact and a single workflow for all calls reduces the number of interactions while improving service quality. The cost savings for the first year was approximately US$8 million, with a possible cost savings over five years of more than US$40 million.

Essential characteristics of a business resilience vendor

Organizations looking to solidify business resilience should carefully consider the capabilities of the vendor(s) with whom they choose to work. A business resilience vendor should be able to provide:

- Global leadership in technical expertise, including broad infrastructure competence and deep, multiplatform technology skills
- Highly responsive, international support for the full scope of IT infrastructure operations, both current operations and operations scoped for near-term and long-term expansion
- Globally consistent services, from simple break-fix to comprehensive, end-to-end support capabilities, so that every location can access immediate expertise to resolve events
- The ability to anticipate problems and provide proactive guidance to meet required service level agreements
- Proof of potential cost savings via outsourced support that may include remote support tools and staff as well as management of contracts, warranties and asset inventories
- Understanding of global business needs and IT strategies, an essential characteristic for organizations focused on maintaining competitive advantage
- Remote and automated tools, which can help control the labor costs of maintaining the IT infrastructure and also speed problem resolution
- Proactive monitoring and event notifications to prevent business disruptions
- Parts replacement capabilities, on time, at the right locations

Assessing risk

An effective business resilience plan must begin with a thorough risk analysis:

- **Rank threats based on past occurrences, the amount of potential revenue loss, damage to the brand, compliance risks and single points of failure**
- **Prioritize safeguards, including provisions for hardware and software support, business continuity and disaster recovery**
- **Conduct a cost-benefit analysis for a quantitative risk assessment**
- **Determine next steps based on threat severity, selected safeguards, and the cost and ease of implementation.**

Take the IBM risk self-assessment

IBM's business resilience capabilities

Through IBM, organizations can obtain all the foundational capabilities needed for a solid business resilience strategy , including business continuity, disaster recovery and hardware and software technical support, that can fully address business-, event- and data-driven risks to the business. In addition, IBM can provide proof of potential cost savings of between 5 and 40 percent, depending on the current state of the support environment and how much support is out-tasked.[8] IBM's depth of expertise—across multiple vendor platforms—and breadth of resilience capabilities are designed to support today's complex IT infrastructures.

For technical support, IBM provides nearly 15,000 technicians and support personnel, 400 parts distribution centers and more than 80 support centers located worldwide, so that organizations can expect responsiveness no matter where they are located, including 24×7 service logistics network availability. For business continuity support, organizations can look to IBM's extensive infrastructure investments; more than 1,800 dedicated business continuity professionals; more than 150 business resilience centers located worldwide; and the depth of knowledge drawn from more than 50 years of business resilience and disaster recovery experience with more than 12,000 disaster recovery clients—all of which has led respected industry analysts to recognize IBM as a leader in business continuity and resilience.

For more information

To learn more about building a foundational business resilience strategy, please contact your IBM marketing representative or IBM Business Partner, or visit the following websites:

- **ibm.com**/services/continuity
- **ibm.com**/services/maintenance

About the authors

Richard Cocchiara
Distinguished Engineer
Business Continuity & Resiliency Services
Global Technology Services

Patrick Corcoran
Global Client Solution Executive
Business Continuity & Resiliency Services
Global Technology Services

Kevin Crowley
Global Sr. Market Segment Manager
Maintenance & Technical Support
IBM Global Technology Services

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
May 2011

[1] 2010 IBM Global IT Risk Study, IBM Institute for Business Value in partnership with the Economist Intelligence Unit.

[2] "IT Failure And Power Challenge UK Business Continuity," *eWEEK Europe*, March 7, 2011.

[3] "eBay Giving Out Coupons and Other Compensation after Website Crash," *MaximumPC*, November 24, 2009.

[4] "Google Mistakes Entire Web for Malware," *The Register*, January 31, 2009.

[5] "Surge Caused Fire in Rail Car," *The Washington Times*, April 2, 2007.

[6] "Software Bug Contributed to Blackout," SecurityFocus, February 11, 2004.

[7] Disaster Recovery Journal and Forrester Research have jointly conducted industry studies for four years. The surveys track changes, trends and future development. Information from the 2011 survey is reprinted in this article with permission.

[8] Savings based on IBM Maintenance and Technology Services customer implementations.

Please Recycle

MTW03008-USEN-01