Proactive technical support: the overlooked essential

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

In the face of rapid and continuous change, business continuity has never been more at risk. Most organizations plan well for backups, data replication and failover to meet continuity and disaster recovery needs. But many business disruptions are due to hardware and software systems failures. Even so, technical support is often overlooked as being essential to business continuity. Best-in-class organizations approach business continuity holistically, by including business continuity, disaster recovery and hardware and software technical support into their business resilience plans.

Business environments are growing more complex every day, and so are the IT systems that support them. The possibility for business disruptions has increased exponentially, as have the ramifications. Yet when planning for business continuity, many organizations overlook the importance of technical support.

Responses to the 2010 IBM Global IT Risk Study—a comprehensive online survey of 556 IT managers and others primarily involved in their business' IT functions—revealed that while 54 percent of respondents said their overall approach to mitigating IT risk was good, only 23 percent believed their organizations were well prepared for hardware and software system failures.[1]

Addressing risk driven by business, events and data

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.

However, many resilience strategies do not effectively and proactively address 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. Uninterrupted business operations, and even ongoing business strategy, hinge on the ability of hardware and software to enable the transformation of data into information. 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.

Redefining the requisite elements of business resilience

Remediation is currently the focus of most organizations' business resilience plans. This focus needs to be expanded to include prevention and maintenance. An operating system without the latest patches and fixes installed can spread a virus to backup servers. Likewise, an older version of microcode on a server can cause failures when new applications are installed. While not as immediately noteworthy as an earthquake, these types of failures can have a significantly greater impact on an organization's daily operations and bottom line.

The good news is that processes and procedures for technical support and maintenance already exist in most organizations—although they are often managed and implemented in a different silo, by different people, than the organization's business continuity and resiliency efforts. The key lies in combining all of an organization's efforts to manage and mitigate business-, event- and data-driven risks into one holistic and cohesive plan.

Foundational business continuity for today's infrastructures

Best-in-class companies are combining planning, prevention (technical support) and remediation (business continuity and disaster recovery) to help solidify ongoing business operations. As part of a holistic business resilience strategy, prevention efforts should include, but are not limited to:

- Hardware maintenance and support for multi-vendor 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.

Beyond foundational resiliency: transferring risk

For risk mitigation, it is sometimes more cost-effective and strategic to transfer risk to a skilled vendor. Managed support, including outsourced infrastructure recovery, auditable compliance and automated tools, can help organizations achieve enhanced IT availability, which in turn supports the continuous availability of business operations.

Organizations seeking to incorporate technical support into their business resiliency and continuity plans may require:
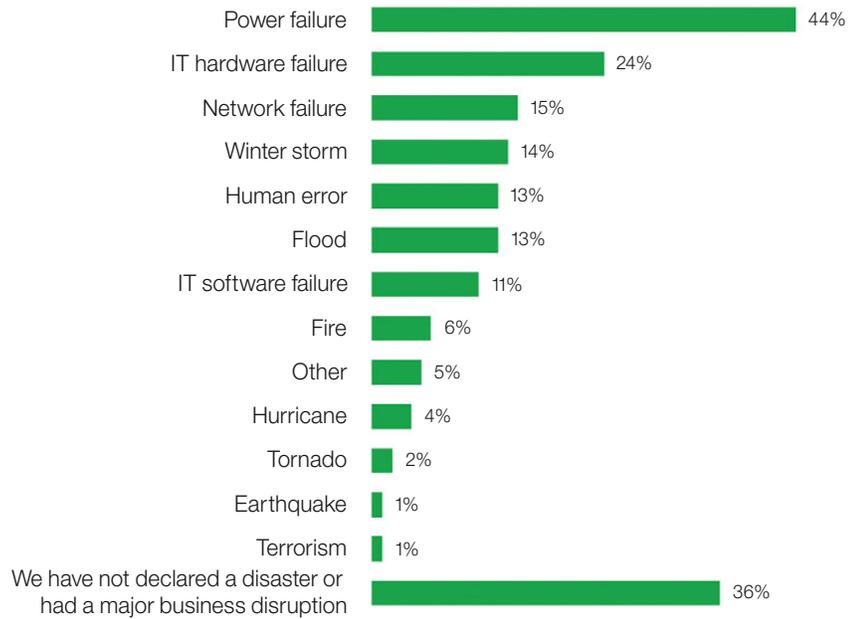
- Holistic support focused on application availability for the end user rather than isolated server and storage availability
- Integrated hardware and software capabilities, including cross-platform and multivendor technical support and proactive microcode and release management, which can help prevent failures and remove complexity
- A single point of accountability across vendors based on consistently agreed upon and continuously monitored service levels
- Proactive monitoring to minimize or eliminate the business impact of technical problems.

How IBM can help

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.[2] IBM's depth of expertise—across multiple vendor platforms—and breadth of resilience capabilities are designed to support today's complex IT infrastructures.

"What is the cause(s) of your most significant disaster declaration(s) or major business disruption?"

Cause	Percentage
Power failure	44%
IT hardware failure	24%
Network failure	15%
Winter storm	14%
Human error	13%
Flood	13%
IT software failure	11%
Fire	6%
Other	5%
Hurricane	4%
Tornado	2%
Earthquake	1%
Terrorism	1%
We have not declared a disaster or had a major business disruption	36%

Base: 200 disaster recovery decision makers and influencers at business globally (multiple responses accepted)
Source: Forrester/Disaster Recovery Journal November 2010 Global Disaster Recovery Preparedness Online

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.

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

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

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

Please Recycle

MTE12345-USEN-01