Building the business case for resiliency

Linking resiliency to business objectives can help IT professionals make a case for corporate investment

How can we convince business executives to invest in resiliency? That's a question that resiliency and continuity professionals ponder every day.

CIOs, business continuity managers and IT managers understand the value of forward-thinking business continuity and resiliency solutions. They know that cloud computing can lower recovery point objectives and recovery time objectives, dramatically improving the availability of data and applications at a time when organizations increasingly depend on the availability of their data and applications. IT leaders understand that they can deploy cloud computing solutions to backup and manage big data, making that information available for business analysis while concurrently accommodating the evolving mandates of Sarbanes-Oxley, the Wall Street Reform and Consumer Protection Act, the European Union's Data Protection Directive, and other governmental and industry regulations worldwide. IT professionals also recognize that secondary data centers and alternate work sites can keep key technologies running, key employees working and critical information continuously available during even the most difficult disruptive events.

But to obtain the support and funding needed to improve business continuity and resiliency operations, IT leaders need sponsorship from C-suite executives who typically focus their attention on overall business goals and bottom-line budget constraints. IT professionals, therefore, find they can generate investment for resiliency initiatives by linking IT risks to business risk—by revealing the critical connections between IT resilience, business strategy and business processes. This process can help convince business executives that the corporation needs highly resilient IT operations to meet its strategic objectives. The IBM Resiliency Services Framework can help in this effort.

The IBM Resiliency Services Framework

The IBM Resiliency Services Framework is a model that helps CIOs, IT managers, business continuity managers (BCMs) and other IT professionals discuss resiliency operations across seven zones of interdependent IT and business operations. These zones are business strategy and vision, organizations and people, processes, applications, data, IT infrastructure and facilities (see Figure 1). Use of the framework can elevate resiliency awareness across the organization. More specifically, it can help IT executives make a compelling case for support and funding by clarifying to business executives the ways in which technology powers the business. The framework can also help IT professionals uncover weaknesses in their resiliency operations, and engender confidence in resiliency operations once those weaknesses have been eradicated.

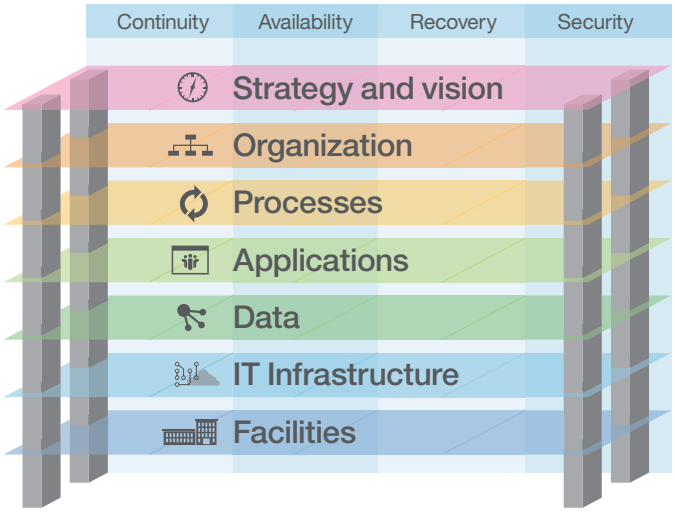

Figure 1. The IBM Resiliency Services Framework helps IT professionals discuss resiliency operations across seven zones of interdependent IT and business operations.

As part of a comprehensive resiliency plan, operations in each zone of the framework must meet industry and corporate standards for continuity, availability, recovery and security. Since these zones are interdependent, each must be examined in terms of its ability to support the others. An internet retailer that can quickly recover its shopping applications after a disruptive event, but not the data that powers them, leaves consumers unable to shop. In this example, the applications and data zones have failed to support each other, and the solution itself has failed to meet the business's objective of providing 24X7 shopping opportunities to its customers. This resiliency failure can also potentially impact the organization's reputation and financial results.

Using the resiliency framework in conversations with business executives helps IT professionals align resiliency investment with overall business strategy. This, in turn, helps IT build a credible business case for support and investment in those areas of an existing resiliency program that are weak enough to pose a risk to corporate objectives.

Examining the framework zone by zone

Strategy and vision

The process starts by developing a clear picture of business objectives. With a little research, IT professionals can gain an understanding of the organization's strategy and vision. Newspaper and magazine articles, interviews with corporate executives, internal communications and corporate web sites can all be sources of information about organizations' business strategy.

For those who work with publicly held companies, annual reports—specifically, the 10-K reports available via sec.gov—make the processes easier. These reports typically list both corporate goals and perceived risks for the coming year. Linking the potential effect of realized risks on corporate goals can do much to engender corporate interest in resiliency operations.

Consider a large retailer that sells through bricks-and-mortar stores and a significant, growing online presence. Under the "Risk" section of its 10-K, the company notes that "If the technology systems that give our customers the ability to shop with us online do not function effectively, our operating results, as well as our ability to grow our e-commerce business globally, could be adversely affected." IT professionals reading this know that their ability to enable the continuous availability of their e-commerce operations, along with their ability to improve recovery point objectives (RPOs) and recovery time objectives (RTOs) of e-commerce applications and associated data, would be of significant interest to the C-suite.

Similarly, a worldwide automobile manufacturer's 10-K may outline its plans to put cutting-edge technology in its cars. The manufacturer also notes that "a security breach of our information technology networks and systems could interfere with our operations and compromise the confidentiality of proprietary information." Anything that IT can do in this situation to protect and restore that information would be important to the C-suite.

Once IT professionals have studied corporate goals and determined which risks the company has identified as threatening those goals, they can use the rest of the framework to determine where additional resiliency investment is needed and gain corporate buy-in.

Organization

The organization zone of the resiliency framework covers employees. It is imperative for IT leaders to embed resiliency into the overall corporate culture: helping each employee to understand the risks that could potentially impact corporate goals, along with his or her role in mitigating them. IT can accomplish this by instituting a risk communications strategy—which may include quarterly newsletters or internal blogs—to regularly inform employees of risk areas and highlight what workers have done to help manage risk.

As part of this zone of the framework, IT should also work with C-suite executives to understand that alternate work space must be secured for key personnel so that they can do their jobs in the event of a disaster. These work sites should include fully-configured, ready-to-use work stations equipped with personal computers, phones, networks, and, if needed, call center capabilities. Emergency work sites also need satellite communications and generators so there is no dependence on local utilities.

Processes, applications

Customer relationship management. Enterprise resource planning. Supply chain management. Sales and communications. These are just some of the universal business processes that are imperative to business operations. Business executives know that. They may not, however, fully recognize the level of dependence between resiliency processes and resilient applications. IT professionals can encourage investment in application resiliency by demonstrating the link between key business processes and the apps that support them.

To start, IT leaders can rank five processes in order of their importance to overall business goals, and list the applications needed to support those processes. IT professionals can then determine the type of resiliency solutions that will quickly recover these applications after a disruptive event. This activity requires identification of the minimum required process functionality, and the identification of alternate processes and procedures that will allow operations to continue during times of stress. Increasingly, organizations are turning to cloud computing for increased automation and improved availability.

Data

How much data is the organization's CEO or CFO willing to lose? What type of data can be lost without hurting revenue or corporate reputation? Without running afoul of government and industry regulations for data availability, privacy or security? Because of well-publicized instances of the consequences of data loss, data backup and protection is the zone of the business resiliency framework in which corporate and IT minds often think most alike. The challenge for IT professionals, then, is to implement the technologies and processes needed to back up and protect data as it is created from multiple, disparate sources, then to quickly restore it after a disruptive event. Ranges of solutions are available to balance cost objectives with recovery point objectives. These include everything from mirrored sites and synchronous data replication to cloud-based backup and recovery operations.

IT Infrastructure

The IT infrastructure zone of the resiliency framework covers the equipment and tools that support the company's business processes and goals—servers, storage systems, networks and mobile devices. Since these technologies power and store applications and data, and keep employees working and communicating, the need for resilient technology should be clear to business executives. Resiliency investments should include funding for redundant and failover/failback technologies. Depending on the size and complexity of the company's IT infrastructure, IT resiliency solutions can include simple hardware replacements, prepackaged recovery technologies shipped to the organization's location of choice after a disruptive event, use of vendors' traditional and cloud-based server recovery, and highly complex mirrored environments.

Facilities

If IT professionals can convince business executives of the value of technology resiliency, the need to find facilities to house backup IT operations should be an easy sell. Resiliency and recovery headquarters should be located far enough away to escape vulnerability to the same risk events—hurricanes, earthquakes, acts of terrorism, as examples—that threaten the primary site, but close enough for employee access. Backup sites should feature communications, power systems, and HVAC systems independent of local utilities, which may be affected by the same disruptive event as the organization itself. The resiliency center may also act as an emergency workspace for key personnel. In these instances, work area recovery stations should be outfitted with the productivity and communications tools discussed under the "Organization" section of this paper.

Why IBM?

Aligning resiliency programs with overall business strategy is a challenging process. Significant and specialized knowledge of the latest resiliency methodologies and technologies is often needed to determine whether each component of a resiliency plan supports the organization's overall business objectives, and how to cost-effectively improve them if they do not.

This complex undertaking can begin simply, with a consultative discussion with IBM to review the resiliency framework with your organization. During this in-person discussion, IBM representatives will evaluate your current resiliency and continuity strategy against the IBM Resiliency Services Framework, assessing each zone in terms of its efficacy and adherence to industry and corporate standards for continuity, availability, recovery and security. This discussion leaves IT professionals with a better idea of which aspects of their resiliency programs support overall business goals and which need improvement.

IBM Resiliency Services can also help with the design, implementation and management of resiliency solutions. IBM Resiliency Services cover every zone of the resiliency framework. Many—including our cloud services for data and application backup and availability, and for server recovery—are offered as managed services, freeing organizations from the capital outlays and staffing burdens required to hone their resiliency programs to meet the challenges of today's threat landscape.

If an organization needs physical recovery sites, our global network of security-rich, fully-equipped business resiliency centers are available for emergency IT operations. They also house fully equipped work area space for key corporate personnel. These resiliency centers help corporations avoid the capital and staffing costs that comes with building, outfitting and operating their own emergency data centers and work sites. If an organization chooses to build its own resiliency site, IBM can help with its design, construction and outfitting. Our services help the organization determine the new site's capacity, availability and security requirements, helping the organization to mitigate risk and improve its business continuity posture. Ongoing support and management services are also available.

With more than 50 years' experience in business continuity and resilience, IBM is an acknowledged market leader and innovator in this field. Our more than 6,600 continuity and resiliency professionals serve more than 10,500 clients. You can find our more than 300 cloud resiliency centers in 68 countries around the globe. Very few organizations operating in the resiliency arena can match our track record, expertise, portfolio breadth and reach. With this experience, we can help IT leaders develop the type of business case for resiliency that will make the C-suite take notice.

For more information

For more about IBM Resiliency services, call 1-877-426-3287. Or visit our web site:
ibm.com/services/us/en/it-services/business-continuity

IBM Corporation
IBM Global Technology Services
Route 100
Somers, NY 10504

Produced in the United States of America
May 2015

BUW03045-USEN-01