



Beyond Disaster Recovery

Protecting Mainframes to Ensure Business Continuity

Table of Contents

- ABSTRACT**..... 1

- INCREASING THREAT TO BUSINESS CONTINUITY**..... 3
 - Driving Factors.....3
 - Resulting Threats3
 - Traditional Methods Come Up Short4

- INTELLIGENT AUTOMATION PROVIDES A SOLUTION**..... 4
 - Minimize Failed Changes to IT Infrastructure4
 - Maintain Service Quality as Conditions Change4
 - Detect and Eliminate Contaminated Data5
 - Preserve Skills of Experienced Mainframe Personnel.....5
 - Ensure Successful and Speedy Recovery from Disasters5

- PART OF A BROADER SOLUTION**..... 5
 - Encompass both Distributed and Mainframe Components 6
 - Support Business Service Management..... 6

- CONCLUSION** 6

About the Author

Bronna Shapiro, director of Solutions Marketing for Infrastructure and Application Management and Mainframe Solutions for BMC, manages a team responsible for solutions marketing strategy and baseline campaigns for BMC. Her prior industry experience is in product management of key mainframe products and as an instructor for courses on IMS and DB2 conducted worldwide.

Abstract

Mainframe systems continue to store the majority of the world's digital information. Because the mainframe is so critical to business continuity, when mainframe data is lost, corrupted, or cannot be accessed quickly, it can be catastrophic to the business. Consider the consequences when a telephone company loses its customer billing data, or when an online brokerage firm's performance degrades so badly that delayed stock trading transactions cause customers financial loss.

Mainframe enterprises must ensure business continuity, keeping the business running in an uninterrupted fashion to meet service level agreements (SLAs) for both availability *and* performance. To do so, these enterprises must protect all aspects of the mainframe ecosystem that supports vital business information.

People typically associate threats to business continuity with disasters such as hurricanes, floods, or terrorist attacks. These calamitous events can wipe out entire data centers, severely disrupting business. Disaster recovery mechanisms have proven their ability to help enterprises struck by disasters quickly get back to business. Consider the fast recovery from the September 11 terrorist attack in New York, and the fact that enterprises along the U.S. gulf coast were able to maintain business continuity despite the recent spate of hurricanes. Such disaster recovery mechanisms also are effective in protecting data when hardware fails.

Other types of events, such as human errors, application errors, and delays in reacting to changing conditions in the mainframe environment, also can disastrously disrupt business continuity. Such events can cause data loss, data contamination, outages of critical IT resources, and degraded performance of key business applications — all with far-reaching business consequences. Companies must be equally prepared to deal with these types of events.

These other events that threaten business continuity are occurring more frequently, for three main reasons:

- > The complexity of the IT infrastructure is high and rapidly increasing.
- > The mainframe has become more intertwined in the fabric of business; more users and systems need access to mainframe information, both inside and outside the walls of the enterprise.
- > The mainframe, like other components of the IT infrastructure, must be available 24x7. This leaves a very small maintenance window at best, forcing the operations staff to perform maintenance while systems are up and running, or in the limited downtime window for those functions that cannot be done while the systems are up and running. This puts greater pressure on the operations staff and opens the door to errors.

IT faces a daunting challenge. The IT staff must protect the mainframe ecosystem to ensure business continuity on a 24x7 basis and in a highly complex open environment that poses an increasing risk to business continuity.

This paper:

- > Examines the risk to business operations and continuity posed by events other than disasters or hardware failures.
- > Describes how solutions based on intelligent automation can mitigate threats to business continuity and significantly increase operational efficiency.
- > Discusses the importance of implementing a business continuity solution in the broader context of Business Service Management (BSM).

Increasing Threat to Business Continuity

Most enterprises have mechanisms in place that protect the mainframe from disasters (whether natural catastrophes, manmade events, or those due to hardware failures). They feel secure that they can maintain business continuity during adverse conditions. This may, however, be a false sense of security if the right processes are not in place to alleviate associated problems.

Additional associated threats to business continuity can be just as disruptive as disasters or hardware failures, and the risk of their occurrence is increasing. These threats are human errors, application errors, and failure to respond to changes in the IT environment in a timely fashion. Human errors can wipe out critical data. Application errors can stuff erroneous data into business-critical databases. A delay in responding to a change, such as a spike in workload, can drag down the performance of a business-critical application. These events pose serious threats to business continuity. According to leading industry analysts, as much as 80 percent of all unplanned downtime is caused by software problems or human error.

While enterprises have put in place adequate protection against disasters and hardware failures, they also must protect the mainframe from the increased risk of human and application errors. They must ensure that the key IT components (applications, transactions, systems, subsystems, network, storage, middleware, and databases) are all up and running when they are supposed to be and at agreed on service levels.

Driving Factors

Three major factors drive the increased risk of human errors, application errors, and delays in responding to changes in the IT environment:

- > Growing complexity of the mainframe environment
- > Wider access to the mainframe through the Internet
- > Need for 24x7 availability in today's world

Gone are the days when the mainframe was monolithic, walled off from the outside world, and accessed only by a small number of skilled IT personnel. Today, the mainframe is a vital and tightly integrated resource in the enterprise IT infrastructure. As part of a complex, multi-tiered, services-oriented architecture, the mainframe must interoperate with a variety of other resources. For example, a single SAP landscape can include mainframes, multiple servers, and hundreds or thousands of database tables. The resulting

complexity has increased the potential for human error and for errant code in applications.

What's more, today's Internet environment has opened up the mainframe to access by thousands, even millions, of outside users — employees, business partners, and customers. In addition, as a vital component of business processes, the mainframe must participate in business-to-business transactions in which it interoperates with systems outside the enterprise, such as those of business partners in supply and distribution chains.

Finally, the mainframe must meet the demand for 24x7 operation in today's global, Internet-based business environment. Maintenance windows have virtually disappeared, forcing operations staff to perform maintenance tasks — such as deploying bug fixes, and upgrading and adding new applications — while the system is operational or in the very limited downtime window for those tasks that cannot be done while the systems are up and running. The resulting higher pressure on the operations staff increases the risk of human error and leaves little time for proactive efforts.

Resulting Threats

The combination of greater IT infrastructure complexity, increased accessibility of the mainframe, and the requirement for 24x7 operation constricts IT capacity to maintain business continuity and meet availability and performance SLAs. This poses a serious threat to the business. Fortunately, this threat can be addressed through processes and technology as described later in this paper.

Enterprise complexity increases the likelihood that people will make operational errors that can cause data loss. Complexity also increases the probability of coding errors in applications, which can result in the contamination of business-critical databases. What's more, complexity makes it far more difficult for the operations staff to react quickly to changing conditions in the IT environment, which can result in performance degradation.

Data loss can bring down critical business applications, interrupting the delivery of business services with serious consequences. When a retail store's point-of-sale system goes down, customers typically leave the store without completing their purchases. When customers looking for online bank loans find that a bank's system is down, they likely will go to another bank's site to get what they need. In today's Internet economy there is little loyalty, and customers will readily defect if their needs for high availability and fast performance are not met.

Contamination that compromises the integrity of a critical database can go undetected. For example, in updating a database, an administrator makes a single keystroke error in a batch update job that causes the update to be performed with the wrong input data set, contaminating critical business data. The applications that rely on this data continue to operate, but with bad data. The problem may go undetected until reported by end users. Bank customers report that erroneous transactions have been made to their bank accounts. Truck drivers for a parcel delivery company report that the dispatching system has sent them to erroneous locations. Think of the business impact of these errors.

Traditional Methods Come Up Short

Traditional data and IT component protection methods, such as backup, recovery, and data mirroring, are not sufficient by themselves to ensure business continuity in the event of human or application errors. Consider, for example, the case of a critical database contaminated by an application that makes an extraneous entry into the database each time a specific type of transaction occurs. Traditional methods simply back up the contaminated data, perpetuating the problem. The application continues to operate with contaminated data, often with unpredictable results.

Moreover, the use of traditional manual system-management methods is no longer viable. Complexity has increased to a level well beyond the capabilities of even the most skilled IT professionals using traditional manual system-management processes. In this complex environment, manual processes pose a high risk of error. In fact, one of the major sources of human error is the use of system-management processes that rely on manual procedures. Manual processes also can cause increased reaction times to changes in the IT environment, posing the risk of performance slowdown. In addition, manual processes are difficult if not impossible to audit, exposing the organization to the risk of regulatory noncompliance.

Intelligent Automation Provides a Solution

To ensure business continuity in today's complex and demanding IT environment enterprises must augment their existing disaster recovery mechanisms and traditional manual system-management processes with coverage that is more complete. Intelligent automation provides an answer.

Intelligent automation consists of software-driven routines that automatically perform IT service management functions and make decisions based on business impact and business policy. Tools and solutions are available today that help enterprises implement intelligent automation in their mainframe environments.

Intelligent automation brings with it several major advantages. It masks the complexity of the IT infrastructure and helps ensure that IT system-management processes are performed in a repeatable, consistent, and timely fashion using best practices. The result is a dramatic reduction in the risk of error. In addition, intelligent automation provides an auditable trail to ensure regulatory compliance.

Minimize Failed Changes to IT Infrastructure

One process that is particularly susceptible to error is the change process. Many enterprises currently approach change in an ad-hoc fashion and use manual procedures. The process is inefficient and prone to errors that could cause outages. In fact, improperly implemented changes are a major source of outages and account for anywhere from 40 to 70 percent of unplanned downtime, according to industry analysts. By automating change processes, such as the change-request approval process, the IT staff can prevent many unnecessary outages.

Intelligent automation helps ensure consistency of the change process by enforcing standardized, best practice processes, such as those identified in the IT Infrastructure Library (ITIL®) guidelines. The result is a dramatic reduction in the number of change failures.

Intelligent automation also increases the speed and efficiency of the change process, freeing valuable time for highly skilled IT staff. This enables the enterprise to reinvest this time on strategic projects that have a much higher impact on the business.

An example illustrates the power of intelligent automation in change management. An automated database administration solution can baseline the system programmatically and then apply a change — all without IT staff intervention. With the baseline in place, if the change did not produce the expected result, the solution can back out the change. The solution would also maintain an audit trail of the process to support regulatory compliance.

Maintain Service Quality as Conditions Change

Traditionally, the IT operations staff has had to respond manually to alerts, addressing problems that could negatively affect system availability or performance. They first must determine the cause of the problem, and then implement a fix. Because of the sheer number of alerts coming in and the complexity of the IT infrastructure, it is challenging for even the most skilled professionals to respond in a timely fashion with the correct fix.

It's time consuming to diagnose and implement fixes. Analysts have said that as much as 70 percent of the time it takes to recover is *think time*. Moreover, a fix may solve the immediate problem, but introduce problems in other areas of the infrastructure. Furthermore, it's difficult to prioritize actions based on potential business impact, so problems typically are addressed on a first-come, first-served basis.

Intelligent automation provides a solution by enabling the operations staff to move quickly to address problems, eliminating the think time associated with manual problem diagnosis and resolution. It leverages system-monitoring tools, keeping a close watch on the environment and responding automatically and immediately to out-of-threshold conditions. Response is intelligent and based on policy and business impact.

With intelligent automation, the IT staff can move proactively to head off problems before system outages occur or performance degrades. For example, assume a system monitor issues an alert indicating that free space for a certain data set has dipped below threshold. The intelligent automation solution steps in, automatically and immediately allocating additional storage capacity from a reserve storage pool. As another example of the power of intelligent automation, assume system monitors indicate that the workload on a Web server supporting online customer ordering has exceeded threshold. Any further increase in workload will result in performance slowdown. Intelligent automation responds by automatically and immediately alleviating the bottleneck. As a result, the Web server maintains business continuity by moving proactively to prevent server slowdown.

Detect and Eliminate Contaminated Data

Traditional approaches to prevent data loss, such as backup, recovery, and data mirroring, do not ensure business continuity in the case of contaminated data. They simply create copies of the contaminated data, perpetuating the problem. Although applications remain in operation, they are now operating with bad data.

Here again, intelligent automation provides a solution through software recovery. It permits the IT staff to quickly identify and back out the contaminated data from the database, and exclude it from the backup process.

Preserve Skills of Experienced Mainframe Personnel

A major problem facing many enterprises today is the diminishing talent pool of IT professionals with mainframe

expertise. That's why it's imperative to use their time most effectively, and to preserve and leverage their knowledge to the fullest extent possible. Intelligent automation addresses this need, as well.

Intelligent automation eliminates mundane, day-to-day, repetitive tasks that soak up much of the mainframe operations staff's valuable time. It provides automated, preprogrammed responses to problems to ensure successful resolutions without requiring IT staff intervention. In addition, intelligent automation preserves the knowledge of mainframe specialists by encapsulating this knowledge into software-driven intelligent automation routines. As a result, mainframe specialists have more time for activity that is strategic to the business, and that adds more business value.

Ensure Successful and Speedy Recovery from Disasters

Backup procedures ensure that critical information is safely stored and available for recovery purposes. Due to the complex interdependencies of the components in the IT infrastructure, however, recovery must be properly sequenced. Bringing back information in the wrong order can result in recovery failure and introduce significant delays into the recovery process.

Intelligent automation can augment in-place disaster recovery mechanisms to automatically synchronize the recovery process with the correct sequence. By doing so, intelligent automation speeds the recovery process, and it ensures success by enforcing the correct recovery sequence. Intelligent automation also can base the recovery sequence on business priorities, recovering the most business-critical systems first.

Part of a Broader Solution

Enterprises need to broaden their perspective when implementing a mainframe business continuity solution. It's important to implement a business continuity solution that addresses the entire IT infrastructure and not just the mainframe. Also, it's important to implement a business continuity solution in the context of a broader Business Service Management (BSM) strategy. BSM strategy is based on enabling enterprises to align IT with goals that are important to the business.

Encompass both Distributed and Mainframe Components

The right solution can present a consolidated view of the entire IT infrastructure — including mainframe and distributed systems — that shows all deployed assets (hardware, software, and network components), their locations, configurations, their associated users (employees, business partners, customers), and their physical and logical interrelationships. This consolidated view not only masks the complexity of the infrastructure but also helps the staff make better informed, intelligent decisions related to business continuity.

Support Business Service Management

IT organizations should approach business continuity in the context of a wider BSM strategy. BSM helps enterprises align IT practices to the goals of the business, merge business with IT information, and ensure that IT is able to support business goals. That's why it's important that the business continuity implementation support BSM concepts.

BSM solutions permit IT to make decisions, including intelligent automation decisions, based on their business impact. To do so requires a solution that is capable of associating the IT infrastructure components with the business services they support, for example, by indicating which servers and databases support which SAP applications.

Moreover, business continuity involves several BSM disciplines, including change and configuration management, service impact and event management, incident and problem management, and infrastructure and application management. As a result, it's vital that the business continuity solution operate in concert with solutions that support these various disciplines.

By implementing a business continuity solution in view of the broader BSM strategy, IT can maximize its contribution to business value.

Conclusion

Most enterprises have mechanisms in place that help protect the mainframe and maintain business continuity in the event of disasters and hardware failures. Today, however, other risks exist that are not adequately addressed by these mechanisms. Human errors, application errors, and inordinate delays in responding to changing conditions in the IT environment all can interfere with business continuity. Any of these factors could cause system outages or performance degradation that interrupts business continuity.

Intelligent automation reduces the risk of human error and mitigates the impact of application errors on business continuity. In addition, it permits the IT staff to move quickly and proactively to address changing conditions before systems go down or performance degrades.

In selecting an intelligent automation solution, it is important to look for one that encompasses not only the mainframe but also the distributed components of the IT infrastructure. In addition, to ensure that business continuity actions are based on business impact, look for a solution that is part of a broader Business Service Management strategy.

With the right intelligent automation solution, an enterprise can move beyond disaster recovery to fully protect its mainframes from a wide variety of adverse events. In so doing, the enterprise can maintain business continuity, delivering business services at agreed on availability and performance levels.

BMC Software provides solutions that help ensure business continuity. For more information, please visit www.bmc.com.



ACTIVATE BUSINESS WITH THE POWER OF IT.™

About BMC Software

BMC Software helps IT organizations drive greater business value through better management of technology. Our industry-leading Business Service Management solutions ensure that everything IT does is prioritized according to business impact, so IT can proactively address business requirements to lower costs, drive revenue, and mitigate risk. BMC solutions share BMC® Atrium™ technologies to enable IT to manage across the complexity of diverse systems and processes — from mainframe to distributed, databases to applications, service to security. Founded in 1980, BMC Software has offices worldwide and fiscal 2005 revenues of more than \$1.46 billion. BMC Software. Activate your business with the power of IT. For more information, visit www.bmc.com.

