



# SteelEye Technology 2006 Business Continuity Index Survey Results

## Abstract

Answered by 184 C-level executives and IT technicians with active roles in their organizations' business continuity strategies, the first annual SteelEye Technology Business Continuity Index examines adoption levels of various server technologies, delves into priorities and costs for implementing Business Continuity (BC) initiatives and provides a view into common BC practices.

Table of Contents

Background .....	3
Methodology .....	3
Results .....	3
Demographics .....	4
Business Continuity Requirements and Planning.....	6
Discussion .....	12
Summary .....	13
About SteelEye Technology.....	14

## Background

In the fourth quarter of 2005 and first quarter of 2006, SteelEye Technology developed and administered a survey to measure the state of business continuity (BC) planning among IT organizations. The survey was designed to gain particular insight into the most disruptive types of IT outages, the causes of IT outages against which respondents felt most important to protect, and the level of implementation of technologies such as data replication and failover clustering within existing BC plans. SteelEye will make the data available for publication as requested by journalists and analysts.

It is planned for this to be the first annual SteelEye BC Index survey, with future results being tracked for changes in BC planning and implementation.

## Methodology

The SteelEye BC Index survey was conducted via a specially designed web portal with logic determining which questions to ask based on prior responses. For example, respondents who indicated that they did not have a BC plan were not asked questions describing components of that plan.

Respondents were solicited via email invitations and articles published promoting the survey. SteelEye partnered with [Continuity Central](#), a leading web portal focused on BC planning, to solicit further responses.

A total of 184 responses were received. Respondents were asked to self-identify on several pieces of demographic information, as detailed in the results section below, for the purpose of comparing responses across industry sector, across geographies, across company sizes, etc. All respondents were identified by an IP address to limit responses to one per unique IP address.

## Results

This section presents each question that was asked as part of the survey and provides summary answers. Select question/response pairs that have revealed interesting information are followed by commentary in the Discussion section. Analysis of responses across geographies, across industry or breakdowns among subgroups can be performed and the resulting data provided on request.

To obtain additional information on the survey results or to schedule discussions on the results presented, contact Bob Williamson, Vice President of Products for SteelEye at [bob.williamson@steeleye.com](mailto:bob.williamson@steeleye.com) or +1-843-532-0355.

## Demographics

Respondents were asked to self-identify based on a set of demographics questions.

### Which choice best describes your position within your organization?

Total responses = 184

<i>Position</i>	<i>Percent</i>
Member of IT staff	53.3
CEO/COO/CIO/CFO (C-Level)	21.7
Head of IT	14.1
Member of Development Staff	6.5
Head of Engineering	4.3

### Which industry sector best describes your organization?

Total responses = 184

<i>Industry Sector</i>	<i>Percent</i>
Finance	18.5
Technology	16.3
Government	7.1
Insurance	7.1
Health Care	6.5
Services	6.5
Communications	5.4
Entertainment and Media	4.9
Education	4.3
Manufacturing	4.3
Retail	3.8
All Others	15.3

**Which choice best describes the number of people in your organization?**

Total responses = 184

<u>Organization Size</u>	<u>Percent</u>
< 50	21.8
50 to 100	7.1
101 to 500	10.3
501 to 1000	13
1001 to 5000	14.7
5001 to 10000	11.4
10001 to 25000	9.2
> 25000	12.5

**What is the geographic location of the majority of the critical IT functions within you organization?**

Total responses = 184

<u>Location</u>	<u>Percent</u>
North America	47.8
Europe	28.8
Asia	13
All Others	10.4

**On which Operating Systems do you run business critical applications?**

Respondents selected all operating systems which were appropriate for their organizations. Total responses = 184

<u>Operating System</u>	<u>Percent</u>
Windows	78.8
Linux	39.7
Solaris	26.1
AIX	21.7
HP-UX	21.2
Netware	6.5
All Others (VMS, Z-OS, Unixware, VMware)	21.2

## Business Continuity Requirements and Planning

Respondents were asked to reflect on their IT infrastructure and their BC requirements.

### Rank these services in importance for your organization to protect as part of a BC plan.

(More Important = 1, ..... Less Important = 5) Total responses = 180

<i>IT Service</i>	<i>Importance</i>
Customer Support	1.6
Corporate Financials	1.7
Email	1.8
Phone System	1.9
Corporate Website	2.4
Order Accept/Delivery	2.4
File and Print	2.6
Manufacture/Product Dev	3.2
Instant Messaging	3.9

### How long could the most important services be unavailable before the downtime becomes a potentially fatal issue for your organization?

Total responses = 181

<i>Length of Time</i>	<i>Percent</i>
Less than 4 hours	32
Between 4 and 8 hours	17.1
Between 8 and 24 hours	23.8
Between 1 day and 1 week	21
Between 1 week and 1 month	4.4
More than 1 month / Unknown	1.7

**Rank these causes of application downtime based on how common they are for business critical applications within your organization.**

(1 = More Common ..... 5 = Less Common) Total responses = 180

<i>Cause of Downtime</i>	<i>How Common</i>
Software Maintenance	2.6
Network Maintenance	2.7
Network Outage	2.7
Application Failure	2.8
Hardware Maintenance	2.8
Hardware Failure	3.0
Power Failure	3.3
OS Failure	3.5
Natural Disaster	4.0
Denial of Service	4.1
Terrorism	4.4

**Rank these causes of unscheduled application downtime based on which would have the greatest impact on your organization's ability to function.**

(1 = More Impact ..... 5 = Less Impact) Total responses = 179

<i>Cause of Downtime</i>	<i>Impact</i>
Network Outage	1.7
Application Failure	1.9
Hardware Failure	2.1
OS Failure	2.2
Power Outage	2.3
Natural Disaster	2.5
Terrorism	2.8
Denial of Service Attack	2.9

**Does your organization have a Business Continuity Plan?**

Total responses = 184

<i>Have BC Plan?</i>	<i>Percent</i>
Yes	73
No	19
Unsure	8

**Organizations that have BC plan**

Respondents who answered that their organization does have a BC plan were asked questions about that plan.

**How often does your organization test its BC plan?**

Total responses = 134

<i>Test Interval</i>	<i>Percent</i>
Daily	2
Weekly	2
Monthly	9
Quarterly	23
Annually	47
Never	5
Other (Biweekly, Semi-annual, ...)	12

**Has your BC plan been invoked as a result of unplanned outage?**

Total responses = 134

<i>BC plan invoked?</i>	<i>Percent</i>
Yes	45
No	52
Unsure	3

**What is the amount of US\$ that organization spends annually on BC plans?**

Total responses = 134

<i>Spends on BC plan</i>	<i>Percent</i>
Less than \$100,000	40.3
\$100,000 to \$250,000	20.1
250,000 to 500,000	8.2
500,000 to 1,000,000	11.2
Over 1,000,000	11.2
Unsure	9

**Does Your BC Plan include a disaster recovery site?**

Total responses = 134

	Percent
Yes	86.6
No	13.4

**Organizations that have disaster recovery site**

Respondents who answered that their organization does have a disaster recovery site were asked questions about that site and the technology used to connect to the site.

**What is the relative location of primary datacenter and disaster recovery site? Total responses = 113**

<i>Location</i>	<i>Percent</i>
Within the same city	29.2
Within the same state	23.9
Within the same country	53.1
Across different countries	7.1

**Is an automated data replication solution part of BC plan?**

Total responses = 113

	<i>Percent</i>
Yes	64.6
No	32.7
Unsure	2.7

**Is an automated failover cluster solution part of BC plan?**

Total responses = 112

	<i>Percent</i>
Yes	35.7
No	53.6
Unsure	10.7

### **Organizations which have BC plan but that plan does not include a remote disaster recovery site**

Respondents who answered that their organization does have a BC plan but that plan does not include a disaster recovery site were asked a question to identify why no remote site has been implemented.

#### **What is the level of importance of each of the possible reasons below as to why your organization has not invested in a disaster recovery site?**

(1 = Most Important ..... 5 = Least Important) Total responses = 19

<u>Reason</u>	<u>Importance</u>
Cost to Implement	2.4
No business requirement	3.1
Priority among IT Projects	3.3
Skills to Implement	4.0

### **Organizations which have do not have a BC plan**

Respondents who answered that their organization does not have a BC plan were asked a question to identify primary reasons why no plan has been implemented.

#### **What is the level of importance of each of the possible reasons below as to why your organization has not invested in a Business Continuity Plan?**

(1 = Most Important ..... 5 = Least Important) Total responses = 32

<u>Reason</u>	<u>Importance</u>
Cost to Implement	2.2
Priority among IT Projects	2.3
Skills to Implement	2.9
No business requirement	3.1

## Discussion

Over three quarters of the respondents (79%) are using Microsoft Windows platforms to host critical IT functions. Linux is being used by approximately half that number (40%) and, surprisingly, surpasses Solaris, AIX and HP-UX in number of implementations.

Interestingly, a significant portion of Windows users also run Linux within their IT shop (39%). This indicates that users are choosing operating platforms which are most appropriate for their IT tasks without concern for maintaining a homogeneous operating environment (56% indicate mixed OS environments). Forty two percent of organizations running Linux also have Solaris deployed within their datacenter while smaller numbers also have AIX (23%) and HP-UX (19%), undoubtedly indicating that a migration from UNIX to Linux is underway as infrastructure is upgraded and additional investments are being made.

Of respondents who answered that only a single OS is used within their critical IT environment (44%), Microsoft Windows was by far the OS of choice (65% versus Linux at 12%).

Despite growing industry-wide adoption of formalized BC plans (73%) and a startling 45% of organizations who have needed to invoke those plans many organizations still fall short in their preparedness for an IT disaster.

Respondents to the survey reported that on average they have less than 8 hours to correct outages before the downtime becomes a potentially fatal issue for their organizations; with the largest number of organizations (32%) reporting anything more than four hours of outage as disastrous. This shrinking window of tolerance for downtime demands the use of automated tools for proactive monitoring, data replication and application failover. Even for companies which may not desire automatic failover of critical applications to a remote site, having a monitoring and alerting mechanism in place can greatly reduce lengths of outages.

Even with this narrow timeline, a surprising 19% of organizations have no plan whatsoever for assuring business continuity, with these enterprises most often blaming cost as the key barrier. But the survey also showed that the biggest slice of organizations (40%) spends less than \$100,000 per year on their BC initiatives. This suggests that organizations who look at cost as a primary barrier to developing a BC plan should revisit the actual costs in relation to their business risk. It is SteelEye's experience that when actual risks are analyzed and dollar values are attached to these risks, that companies find it very simple to cost justify the implementation of a BC plan.

This research clearly demonstrates that a good business continuity plan is by no stretch reserved for organizations with huge budgets. When you consider how many organizations actually use their BC plan, and that any company without one could be just a day or two from a 'fatal issue,' the real costs for business continuity assurance begin to look miniscule.

More encouraging findings reveal not only that 73% of organizations have formalized BC plans in place, but also that 87% of those plans include a remote disaster recovery site as a failover option.

Yet even organizations with a plan may be slow to adopt best practices associated with business continuity assurance.

For example, although 95% of organizations test their BC plans at least annually, organizations that have needed to invoke their BC plans test their plans more than twice as often as those who have not yet encountered a potential disaster (19 times per year vs. nine). This suggests that many organizations seriously underestimate the likelihood of a disaster, and that only once they experience a threat do they prioritize testing as a regular practice.

In addition, while a majority (65%) of organizations with BC plans have implemented an automated data replication solution between their primary and disaster recovery sites, the majority (54%) have not yet implemented an automated failover cluster solution, seen by experts as another key component in a comprehensive business continuity plan.

Using a 1-5 scale (1 being most important), respondents rated protecting customer-centric and communication-oriented services including customer support (1.6), email (1.8), phone system (1.9) and corporate website (2.4) as most critical. Less critical is assuring uptime of operational applications such as file/print services and manufacturing and product development. Instant messaging was by far the least important service to protect indicating its role as a non-critical communication mechanism within corporations today.

Maintenance activities account for three of the top five causes of application downtime within organizations with software (2.6), network (2.7) and hardware (2.8) maintenance all among the most common. This indicates that managing these planned outages should be as important to ensuring business continuity as protecting against unplanned outages.

## **Summary**

The SteelEye Business Continuity Index confirms that BC planning is a critical function within IT organizations of all size and indicates that BC plans can be implemented and maintained for under \$US 250,000 per year in most cases. The protection of customer-focused and communications-oriented services is ranked as most important among corporate functions with recovery in less than four hours seen as vital to their business by one-third of respondents.

Companies point to planned maintenance activities accounting for the largest reasons of application downtime indicating that a solution which can protect against both planned and unplanned outages is ideal.

This is the first annual survey focusing on business continuity planning and implementations among a world-wide sampling of IT organizations. Future surveys will gather data for historical comparison as well as expanding include questions on the use of emerging technologies such as server virtualization.

## About SteelEye Technology

SteelEye is a leading provider of data and application availability management solutions for business continuity and disaster recovery. The SteelEye LifeKeeper family of application-focused data replication, high availability clustering and disaster recovery solutions are easy to deploy and operate, and enable enterprises of all sizes to ensure continuous availability of business-critical applications, servers and data.

SteelEye has specialized solutions which can monitor and protect any application environment. Off-the-shelf solutions are available for Oracle, MySQL, PostgreSQL, DB2, Sybase, Websphere MQ, IBM Director, Rational ClearCase, SAP Netweaver, Apache, Sendmail, Exchange, SQL Server among others on Linux and Windows. Applications for which SteelEye does not have a pre-built offer can easily be protected using LifeKeeper Extender, a framework for placing applications under LifeKeeper protection.

To complement its software solutions, SteelEye also provides a full range of high availability consulting and professional services to assist organizations with the assessment, design and implementation of solutions for ensuring High Availability within their environments.

SteelEye and LifeKeeper are the winners of numerous industry awards including LinuxWorld 2005 "Best Clustering Solution", SAP Pinnacle Award for Outstanding Product Development and 2005 Windows IT Pro Reader's Choice Award.

To learn more about SteelEye, visit [www.steeleye.com](http://www.steeleye.com).

### Trademark Notice

SteelEye Technology, SteelEye and LifeKeeper are registered trademarks of SteelEye Technology, Inc. All 3rd party trademarks are the property of their respective owners.