
The Vulnerability Index®

Trends in Enterprise Vulnerability to Disasters and Disruptions
Wave Four — 1999

A Research Report Prepared For:



Co-sponsored by:

BellSouth and Oracle

October 1999

Table of Contents

- Introduction** **1**
 - Background and Purpose1
 - Research Objectives.....2
 - Research Method2
 - Reading Notes.....3
- Summary of Findings** **4**
- Conclusions** **9**
- Detailed Findings** **11**
 - Enterprise Vulnerability and Preparation for Disruption.....11
 - Internet, Intranets and Extranets18
 - Business Continuity Planning.....20
 - Benchmarking Business Continuity.....26
 - Backup and Data Storage Procedures.....29
- Profile of Respondents** **31**
 - Organization Profile.....31
 - Executive Profile.....32

Introduction

Background and Purpose

In 1993, Comdisco released a study that measured the degree to which large computer users are vulnerable to disasters and disruptions that limit access to the systems and data they need every day. That study revealed that a substantial portion of organizations that depend on their computer systems for day-to-day operations was extremely vulnerable to these interruptions. Local area networks were particularly vulnerable if one of these disasters struck.

In the six years since that initial study was released, a number of significant changes occurred:

- A number of disasters took place that demonstrated the need for preparation in event of these occurrences. These events ranged from natural disasters such as earthquakes, hurricanes, flooding as well as normal disruptions that occur every business day including power outages and hardware failures.
- A continuing increase in the use of local area and the dramatic growth of wide area networks.
- The explosive commercial growth of the Internet, intranets and extranets.

As a result of these developments, there is a continuing concern that many businesses that depend on technology to run their business remain unprepared in event of a disaster or disruption.

Research Objectives

Because of this ongoing concern, Comdisco and its co-sponsors BellSouth and Oracle commissioned *The Vulnerability Index*®. As in the earlier research, this study sheds light on how well prepared companies are in the event of disruptions or lack of access to computer systems, data and applications.

This study was designed to determine:

- Existence of formal plans in the event of a major disruption to networked or distributed computer systems and related work areas
- Systems, functions and procedures included in formal plans
- Data backup and storage procedures

Also included in the questionnaire was a series of demographic questions used to classify respondents for analytic purposes.

Research Method

Two hundred telephone interviews were conducted among a sample of the largest computer users in the United States. Included in these 200 interviews are businesses, federal, state and local government agencies and non-profit organizations. These respondents were screened for the following functions in their organization:

- Administration of computer and information systems for organization
- Determination of computer and information systems needs for organization
- Approval of computer consultants
- Approval or selection of manufacturers of computer hardware and/or software
- Responsibility for Business Continuity

To insure comparability of this data with the benchmark survey, core questions used in the original study and the sample source remained unchanged. In addition, all data from the current study was weighted to match the same distribution of industry types included in the earlier research.

A profile of respondents appears as an appendix to this report.

Reading Notes

- Percentages read across when % signs appear in left-hand columns.
- Percentages read down when % signs are at the top of columns.
- Throughout the report, — signifies any value less than ½%.
- Where percentages add to more than 100% (*or total shown*), it is due to multiple answers.
- Where percentages add up to less than the total or less than 100%, the differences are due to the exclusion of the "don't knows" and "no answers."
- Sometimes where figures do not add to the totals shown, differences are due to “rounding” the percentages.
- The Vulnerability Index refers to an analysis of specific questions. The score each respondent could receive for its enterprise and application servers, local area network, wide area network or Internet, ranged from zero (*minimum vulnerability*) to 100 (*maximum vulnerability*).
- Throughout the report, enterprise and application servers refers to mainframe computers and distributed, UNIX and NT systems. LANs refers to local area networks. WANS refers to Wide area networks.
- Internet includes Internet, intranet and extranet use.

Summary of Findings

Enterprise Vulnerability and Preparation for Disruption

The likelihood that American businesses could be struck by major disruptions to their enterprise computing systems continues.

The *Vulnerability Index* — a measure of preparedness in the event of disruption to enterprise computer systems and data — continues to find that most organizations remain inadequately prepared for recovery in the event of a disruption. In fact, the likelihood of these disruptions is increasing with the explosive growth of the Internet as a form of electronic commerce and service. Clearly, it has never been as important for businesses to protect the availability of their mission critical systems and applications in order to protect revenues as well as their reputation with customers, shareholders and the general public.

The *Vulnerability Index* identified the Internet — *possibly the most important development in business computing* — as particularly vulnerable in the event of a disruption. Among organizations participating in this study, the average *Vulnerability Index* score for the Internet — and related systems functions — is 66. Meanwhile the vulnerability for local area networks has improved somewhat to 55 after remaining stable since 1995. The average index score enterprise and application servers (formerly data centers) remains a surprisingly high 42, a rating that is statistically unchanged from the 1993 index of 46, the 1995 index of 39 and the 1997 index of 43.

Compounding this situation is that very few companies have effective business continuity programs in place to protect the availability of their systems and applications.

Despite the relatively low *Vulnerability Index* for enterprise and application servers, only one in three (39%) companies have an effective business continuity program in place for these systems. This is only a marginal improvement over 1997 when 35 percent of companies had an effective business continuity program in place.

Further complicating this situation is that only one in four (28%) have taken the necessary precautions with their local area networks. As with the overall business continuity score for LANs, this shows an improvement from the one in five (21%) companies who had effective business continuity plans in place for these systems in 1997.

Wide area networks are significantly better prepared than local area networks in the event of a disaster, with 36 percent having an effective plan in place. However, even this level of preparation is inadequate when the overall amount of reliance on these systems is taken into consideration.

Internet-related business functions, however, are the least prepared in event of a disaster or a disruption.

Internet, intranet and extranet-related functions have the highest level of overall vulnerability. This low level of preparation is reflected in the fact that only one in seven of those with Internets (14%) have an effective Internet business continuity plan in place.

The overall vulnerability of networked computers remains high.

In 1993, 42 percent of organizations with LANs received a *Vulnerability Index* score of 100, or total vulnerability in the event of a disaster. Today, the number of organizations with the same degree of vulnerability is about half that level. Close to one in four LANs (22%) is still totally vulnerable in event of a disaster. This compares to 17 percent of LANs that were completely vulnerable in 1997.

Internet, Intranets and Extranets

One in three companies with Internets have not taken any precautions in the event of a disaster.

Thirty-three percent have not taken any of the critical actions needed in order to recover in the event of a disaster that affects their Internet-related business functions. Just as important is the fact that not more than six in ten (58%) of

companies have taken any specific actions. The most common of these actions is management of short-term outages. However, other critical elements such as data synchronization, multiple ISPs and testing & evaluation programs are much less likely to be used.

Many large computer users are actively using their Internets for mission critical business applications.

Thirty-five percent of companies are using Internets as part of their mission critical business functions. With the significant amount of organizations depending on Internets for mission-critical applications, and considering the publicity surrounding the outages of several well-known companies it is surprising that more organizations aren't taking precautions to protect the availability of these applications.

Business Continuity Planning

Nearly one third of organizations do not have a formal business continuity program in place.

Thirty percent of companies do not have a formal program in event of a major disruption or inability to gain access to their computer systems. This compares to the 1997 Vulnerability Index where fewer than half of companies had a formal plan in place. Then, only 45 percent claimed they had a plan. Nonetheless, the number of organizations vulnerable to a business interruption remains excessively high.

The presence of a formal business continuity program significantly decreases overall levels of computer vulnerability.

Among those companies without formal programs, the average *Vulnerability Index* scores were 175 percent higher for enterprise and application servers, 79 percent higher for local area networks, 114 percent higher for wide area networks and 34 percent higher for the Internet. This difference is even more pronounced than it was in 1997 when enterprise and application server vulnerability for companies without plans was 137 percent higher and for local area networks where the difference was 54 percent.

As might be expected, enterprise and application servers are most likely to be included in business continuity programs, with 90 percent of those with formal programs including these systems. Seventy percent include their local area networks and, 72 percent include their wide area networks.

One in four companies have experienced a disaster.

One in four (26%) of organizations participating in this survey have experienced a disruption of or inability to access computer systems. Among these companies that experienced a disruption, 25 percent report having a disruption of more than 24 hours.

The ongoing high degree of work area vulnerability is a result of organizations continuing to ignore some of the most critical elements of business continuity planning.

Only slightly more than half of organizations with enterprise and application servers and about four in ten organizations with LANs have a written set of programs or requirements for the two most critical elements of a Business Continuity plan.

- Designation of alternative sites to relocate to in event of a disruption
- Having a testing and evaluation program for a recovery plan

Companies have significantly increased their allocations for business continuity.

In 1997, 21 percent of companies did not have a budget for this function. Currently, only four percent of companies say they do not have a budget for Business Continuity. Accordingly the average Business Continuity budget has increased from, 6.6 percent of IT budgets to 8.2 percent today.

Benchmarking Business Continuity

Nearly half of the organizations surveyed require 99 percent or greater availability of applications.

Forty-six percent of companies' applications require applications to have 99 percent availability, yet few have the business continuity measures in place to ensure this level of availability.

Few companies have validated their recovery time and point objectives.

Companies typically look for a recovery time objective (downtime) of between four and 24 hours. One in five companies are even more rigorous, looking for a recovery time objective of less than four hours. They take a more stringent view in their recovery point objectives (point of data loss) with one in four companies saying they can tolerate no loss of data under these circumstances. Not

surprisingly, those companies in financial services are much more likely to set rigorous standards in these areas.

However, just over half of those with enterprise or application servers have validated recovery time and point objectives for these systems and only about four in ten have taken the same precautions with their local area networks. Only 44 percent have validated recovery point objectives for their wide area networks.

Backup and Data Storage Procedures

The vast majority of America's largest companies continue to follow rigorous data backup procedures.

In about nine out of ten instances the standard procedure is at least one daily backup of the data stored on the system. The frequency of following these standard backup procedures for enterprise and application servers remains unchanged since 1993.

The frequency of backups for LANs, on the other hand has increased significantly. Today, seven in eight (87%) organizations use a continuous or daily backup as their standard backup procedures for their LANs. This compares to 74 percent in 1997. Overall 96 percent of LAN users follow some standard backup procedure for their systems. This is a significant increase since 1993 when only 45 percent of organizations with LANs used a continuous or daily backup procedure.

Less than two-thirds of companies use automated electronic backup systems.

Only 63 percent of companies are using these systems for their enterprise and application servers. Local area networks — *traditionally the most vulnerable corporate computing system* — are only somewhat more likely to be protected by these systems. Overall, 71 percent of LANs have automated electronic backups in place. This compares to 80 percent in 1997.

Conclusions

Based on these findings, Comdisco has reached the following conclusions from this year's *Vulnerability Index*.

As technology continues to evolve at an incredible rate, businesses' dependence on it grows at a proportional rate. Organizations no longer depend on technology to merely support their business, increasingly it is the foundation of their services.

Businesses can no longer afford to neglect the continuous availability of their enterprise, application servers and data.

Six years after conducting the first Vulnerability Index, we continue to maintain that enterprise, application server and data availability is not getting the crucial attention it needs, in fact the situation has worsened. The following are key reasons:

- The growth of the Internet for communications and for transactions
- The growth of wide area networks
- The shift to enterprise and application servers

With a disruption likely to prevent access to critical data for up to hours and potentially contributing to the loss of profits, protecting technology availability in the form of a business continuity program is critical. This is most clearly demonstrated in the fact that even companies with business continuity plans in place are just as likely to suffer a disruption, the overall length of these disruptions are dramatically shorter.

The twelve basic procedures that computer users should follow in order to minimize disruptions and data loss include:

- Naming a crisis management team with clearly delineated responsibilities

- Estimating the cost of a disruption
- Creating an ongoing system for preventing or reducing the likelihood of a disruption
- Identifying critical information
- Offsite computer data storage
- Recovering critical information
- Designating an alternative site to relocate to in the event of a disruption
- Establishing procedures for communicating a plan within the organization
- Planning for evacuation and transportation of key people and materials
- Having a command center for continuing operations
- Identifying necessary support staff
- Having a testing and evaluation program for a recovery plan

In addition, businesses should adhere to the following the fundamental system characteristics associated with effective business continuity planning:

Wide Area Networks

- Alternate WAN transport
- Process for identifying single points of failure
- Management of short term outages
- Testing and evaluation
- Detailed written procedures
- Local server replication
- Redundant routers

Internets, Intranets and Extranets

- Alternate network access
- Ongoing system for preventing single points of failure
- Management of short term outages
- Testing and evaluation program
- Detailed written plan
- Local server replication
- Redundant routers
- Data synchronization
- Multiple ISPs or multi homing

Detailed Findings

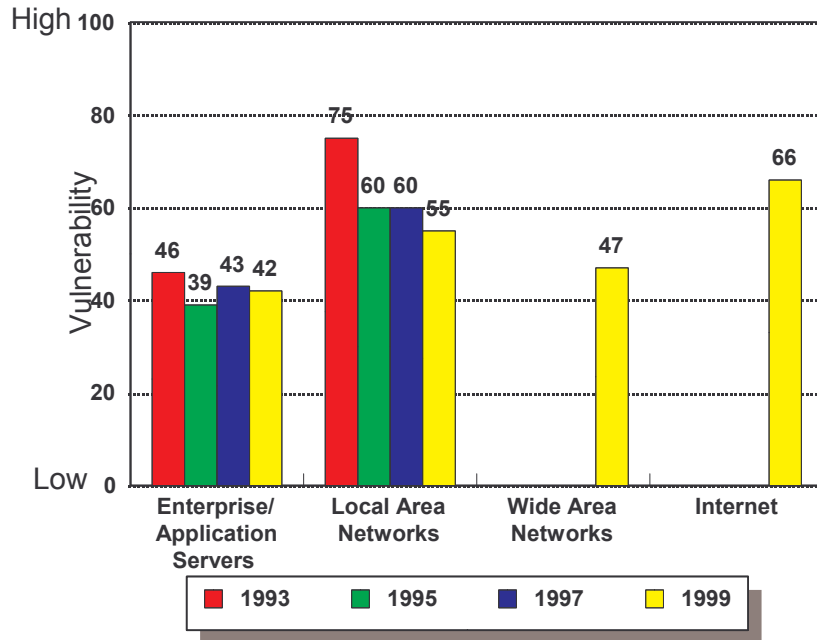
Enterprise Vulnerability and Preparation for Disruption

The likelihood that American businesses could be struck by a major disruption to their enterprise computing systems continues.

The *Vulnerability Index* — a measure of preparedness in the event of disruption to enterprise computing systems — continues to find that most organizations remain inadequately prepared for recovery in the event of a disruption. In fact, the likelihood of these disruptions is increasing with the explosive growth of the Internet as a form of electronic commerce. Clearly, it has never been as important for businesses to protect the availability of their mission critical systems and applications in order to protect revenues as well as their reputation with customers, shareholders, and the general public.

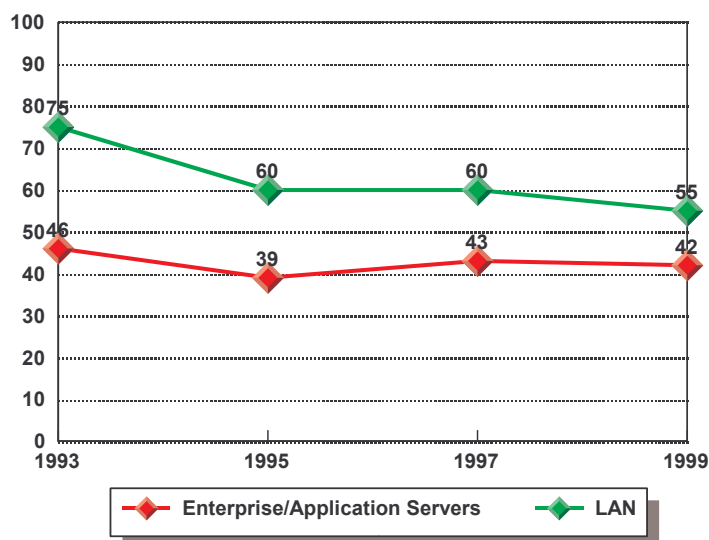
The index measures preparedness for disruptions on a scale of zero to one hundred for local area networks, enterprise and application servers (*mainframes, mid-range computers with distributed terminals*) that are typically linked through wide area networks. **The higher the index, the more vulnerable computer systems are to disruption and disaster.**

Vulnerability Index Scores



The *Vulnerability Index* identified the Internet — *possibly the most important development in business computing* — as particularly vulnerable in the event of a disruption. Among organizations participating in this study, the average *Vulnerability Index* score for the Internet is 66. Meanwhile the vulnerability for local area networks has improved somewhat to 55 after remaining stable since 1995. The average index score for enterprise and application servers computers (formerly data centers) remains a surprisingly high 42, a rating that is statistically unchanged from the 1993 index of 46, the 1995 index of 39 and the 1997 index of 43.

Vulnerability Index Score Trend 1993 to 1999



The index for enterprise and application servers and local area networks consists of a detailed analysis of twelve basic procedures that computer users should follow in order to minimize disruptions of computer systems and related work areas. These basic procedures include:

- Naming a crisis management team with clearly delineated responsibilities
- Estimating the cost of a disruption
- Creating an ongoing system for preventing or reducing the likelihood of a disruption
- Identifying critical information
- Offsite computer data storage
- Recovering critical information
- Designating an alternative site to relocate to in the event of a disruption
- Establishing procedures for communicating a plan within the organization
- Planning for evacuation and transportation of key people and materials
- Having a command center for continuing operations
- Identifying necessary support staff
- Having a testing and evaluation program for a recovery plan

In addition, the enterprisewide *Vulnerability Index* takes into consideration the preparations companies have made in the event of disruptions to their wide area networks and their Internets. These preparations include:

Wide Area Networks

- Alternate WAN transport
- Process for identifying single points of failure
- Management of short term outages
- Testing and evaluation
- Detailed written procedures
- Local server replication
- Redundant routers

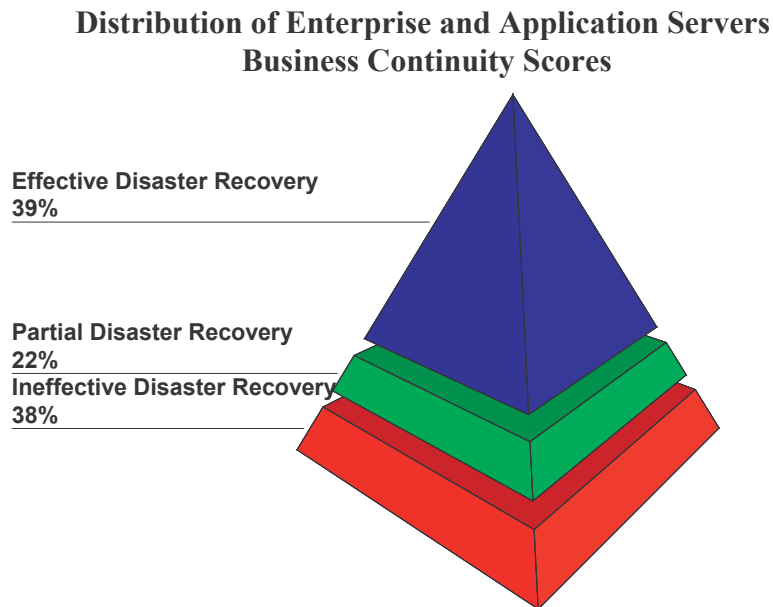
Internets, Intranets and Extranets

- Alternate network access
- Ongoing system for preventing single points of failure
- Management of short term outages
- Testing and evaluation program
- Detailed written plan

- Local server replication
- Redundant routers
- Data synchronization
- Multiple ISPs or multi homing

Compounding this situation is that very few companies have effective business continuity programs in place to protect the availability of their systems and applications.

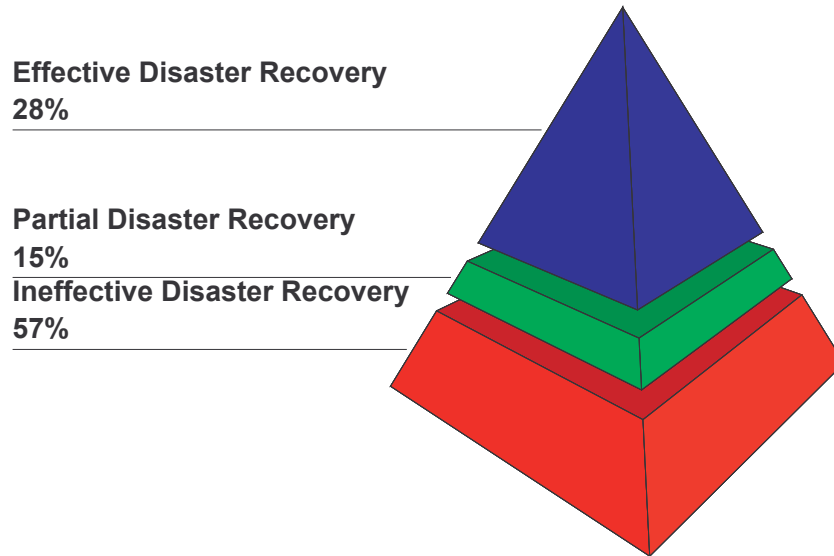
Despite the relatively low *Vulnerability Index* for enterprise and application servers, only one in three (39%) companies have an effective* business continuity program in place for these systems. This is only a marginal improvement over 1997 when 35 percent of companies had an effective Business Continuity program in place.



Further complicating this situation is that only one in four (28%) have taken the necessary precautions with their local area networks. As with the overall business continuity score for LANs, this shows an improvement from the one in five (21%) of companies who had effective business continuity in place for these systems in 1997.

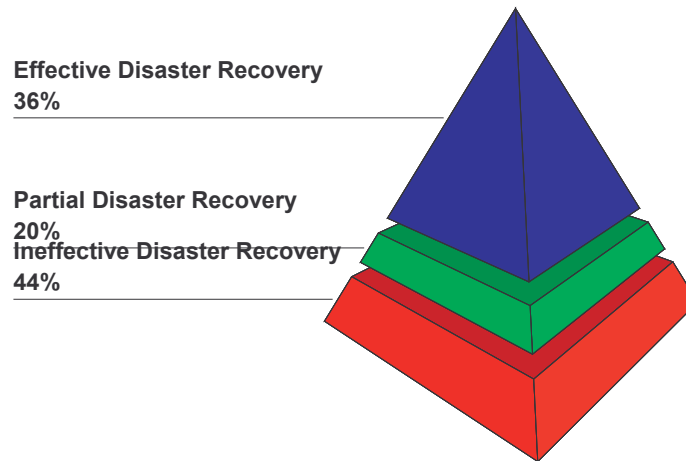
* Effective disaster recovery is defined as a *Vulnerability Index* score of 20 or lower. Partial disaster recovery is an index score of 50 to 79. Ineffective disaster recovery is a score of less than 50.

Distribution of Local Area Network Business Continuity Scores



Wide area networks are more prepared than local area networks in the event of a disaster, with 36 percent having an effective plan in place. However, even this level of preparation is very inadequate when the overall amount of reliance on these systems is taken into consideration.

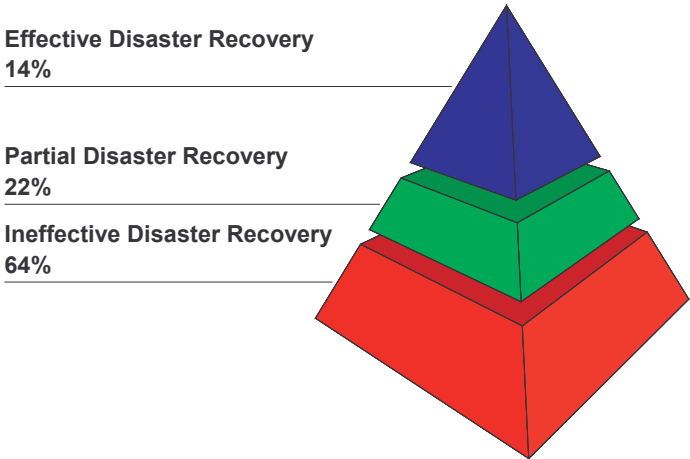
Distribution of Wide Area Network Business Continuity Scores



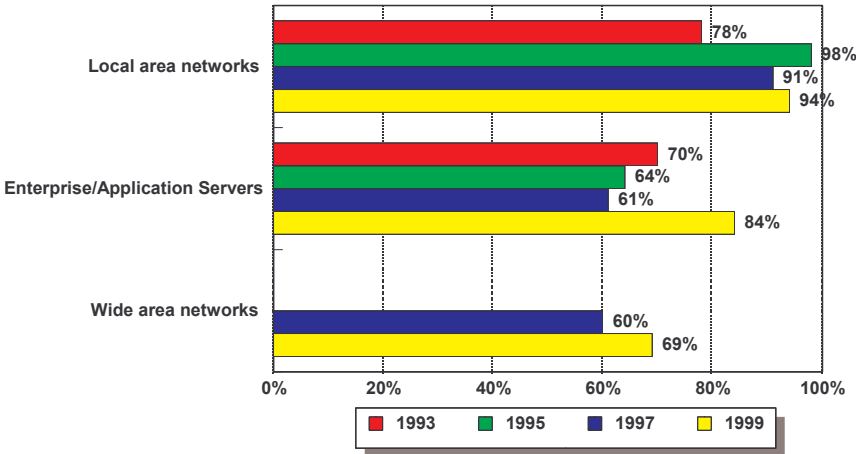
Internet-related functions, however, are the least prepared in event of a disaster or a disruption.

Internet-related functions have the highest level of overall vulnerability. Not surprisingly, this low level of preparation is reflected in the fact that only one in seven of those with Internets (14%) have an effective* Internet business continuity plan in place.

Distribution of Internet Business Continuity Scores



Types Of Computer Systems Used†



With the advent of wide area networks (69% of respondents), many organizations are returning to a model that includes centralized or enterprise computing as part of its systems.

* Effective disaster recovery is defined as a *Vulnerability Index* score of 20 or lower. Partial disaster recovery is an index score of 50 to 79. Ineffective disaster recovery is a score of less than 50.

† Enterprise and application servers statistics from 1993 to 1995 are an average of “centralized mainframes” as well as “mainframe or midrange with distributed terminals”. Statistics from 1997 are based on “enterprise and application servers systems including mainframe and midrange systems”. In 1999, statistics for enterprise and application servers are based on “enterprise and application servers.”

However, the strong emergence of wide area networks along with enterprise and application servers add another level of vulnerability to computing systems that may eventually overshadow the liabilities that already exist with more established computing systems.

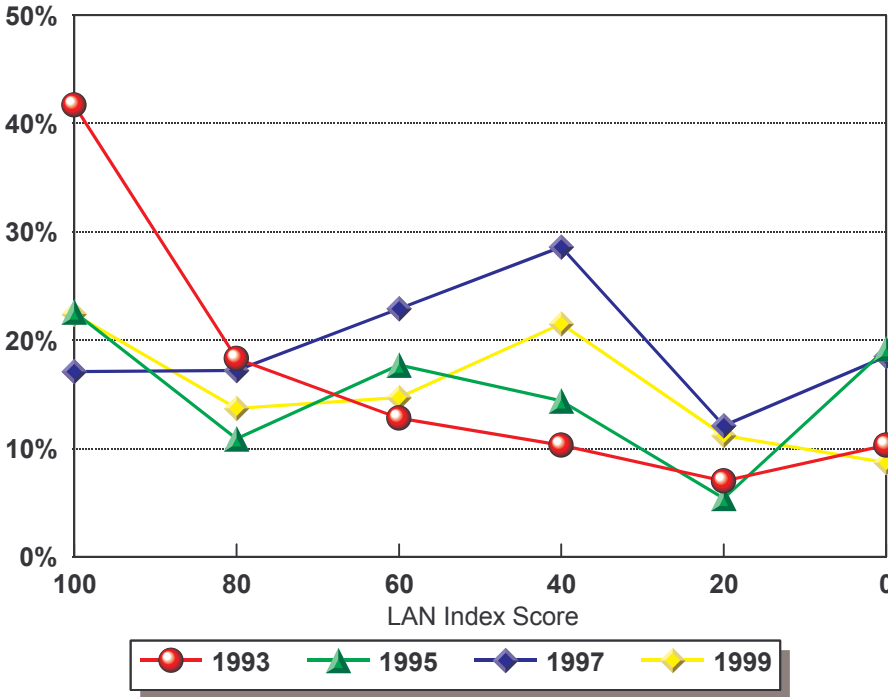
The average vulnerability score for these systems is relatively on par with enterprise and application servers or enterprise systems (*47 for wide area networks versus 42 for enterprise and application servers*). However, the potential vulnerabilities, due to the strong links between these systems, are actually significantly higher than they appear on the surface.

As we noted in the 1997 *Vulnerability Index*, with the number of companies migrating toward enterprise-wide computing systems increasing, the overall level of corporate-wide computer vulnerability will continue to increase geometrically.

Overall vulnerability of networked computers remains high.

In 1993, 42 percent of organizations with LANs received a *Vulnerability Index* score of 100, or total vulnerability in the event of a disaster. Today, the number of organizations with the same degree of vulnerability is about half that level. Close to one in four LANs (22%) is still totally vulnerable in event of a disaster. This compares to 17 percent of LANs that were completely vulnerable in 1997.

Distribution of LAN Vulnerability Scores



However, with the increased shift to wide area networks, the links between these systems increases levels of vulnerability even further. Only 36 percent of wide area networks are adequately prepared for a disaster with only 28 percent of LANs having an equal level of preparation. With the increased linkage of these

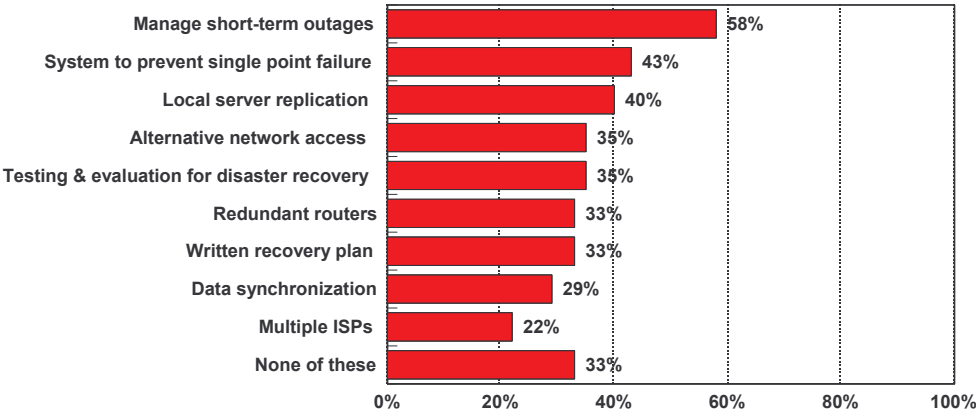
systems for corporate computing, overall system wide computer vulnerability will continue to increase.

Internet, Intranets and Extranets

One in three companies with Internets have not taken any precautions in the event of a disaster.

Thirty-three percent have not taken any of the critical actions needed in order to recover in the event of a disaster that affects their Internet-related business. Just as important is that not more than six in ten (58%) of companies have taken any specific actions. The most common of these actions is management of short-term outages. However, other critical elements such as data synchronization, multiple ISPs and testing & evaluation programs are much less likely to be used.

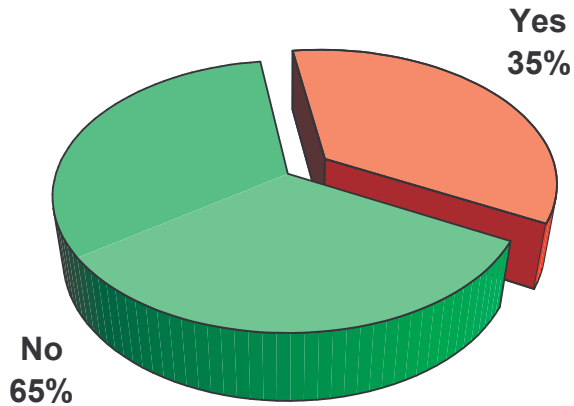
Critical Procedures of Internet Business Continuity Plan



Many large computer users are actively using their Internets for mission critical business applications.

Thirty-five percent of companies are using the Internet as part of their mission critical business functions. With the significant amount of organizations depending on Internets for mission-critical applications, and considering the publicity surrounding the outages of several well-known companies, it is surprising that more organizations aren't taking precautions to protect the availability of these applications.

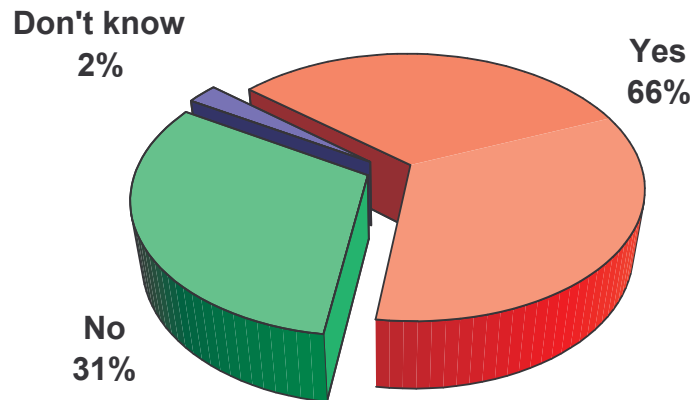
Company Uses Internets For Mission Critical Applications



This is equivalent to 1997 when 37 percent of companies used the Internet for this purpose.

Even more significant is that this initial use of these systems for mission critical applications is only the “tip of the iceberg” in an examination of the long-term opportunity that companies see through the use of these systems. While one in three already use these networks for key applications, two thirds (66%) believe they will eventually be using the Internet as a vehicle for conducting electronic commerce.

Company Plans To Use Internet For Electronic Commerce



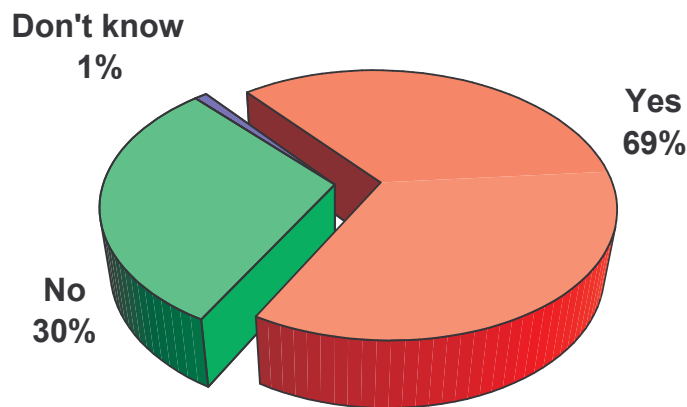
This is a significant increase over 1997 when 49 percent of companies intended to use the Internet for this purpose.

Business Continuity Planning

Nearly one third of large computer users do not have a formal business continuity program in place.

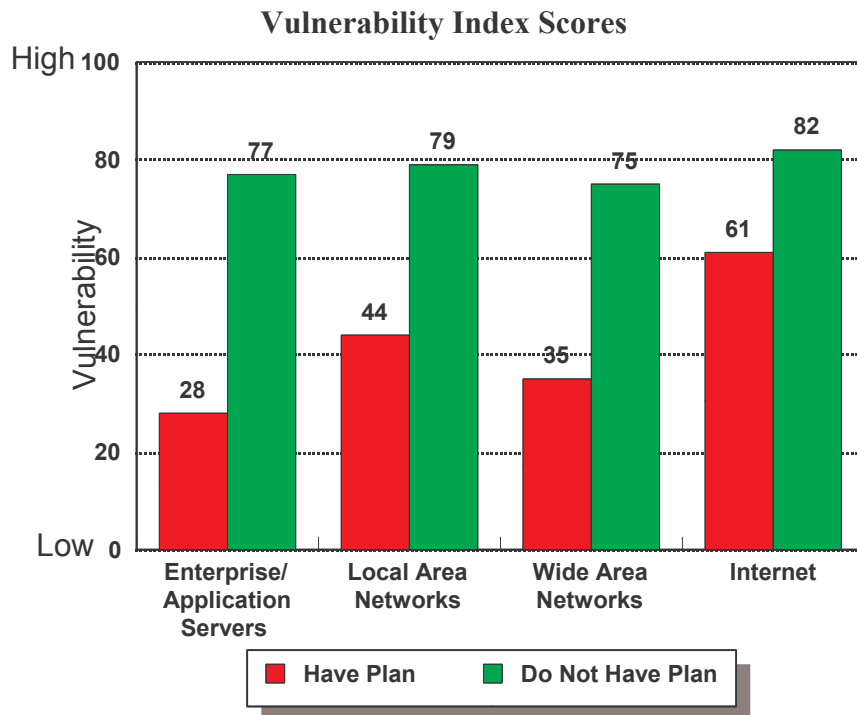
Thirty percent of companies do not have a formal program in event of a major disruption or inability to gain access to their computer systems. In 1997, only 45 percent claimed they had a plan. Nonetheless, the number of organizations vulnerable to a business interruption remains excessively high.

Does Company Have Formal Plan In Event of Computer Disruption?



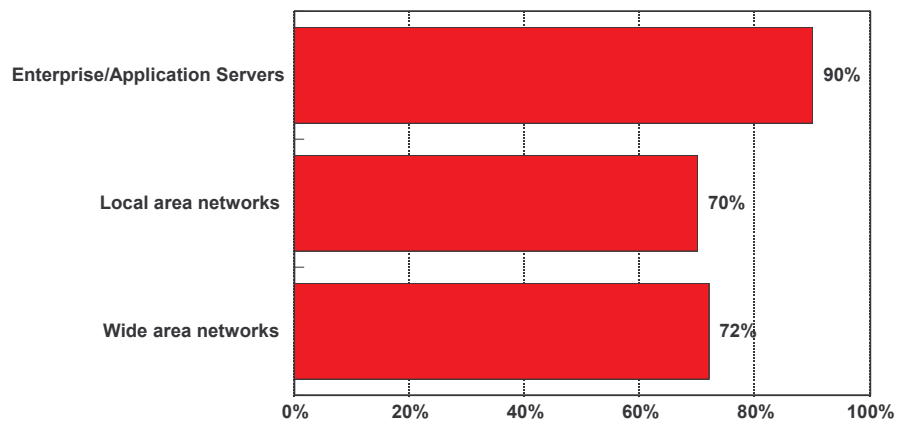
The presence of a formal business continuity program significantly decreases overall levels of computer vulnerability.

Among those companies without formal programs, the average *Vulnerability Index* scores were 175 percent higher for enterprise and application servers, 79 percent higher for local area networks, 114 percent higher for wide area networks and 34 percent higher for the Internet. This difference is even more pronounced than it was in 1997 when enterprise and application server vulnerability for companies without plans was 137 percent higher and for local area networks where the difference was 54 percent.



As might be expected, enterprise and application servers are most likely to be included in business continuity programs, with 90 percent of those with formal programs including these systems. Seventy percent include their local area networks and, 72 percent include either their wide area networks.

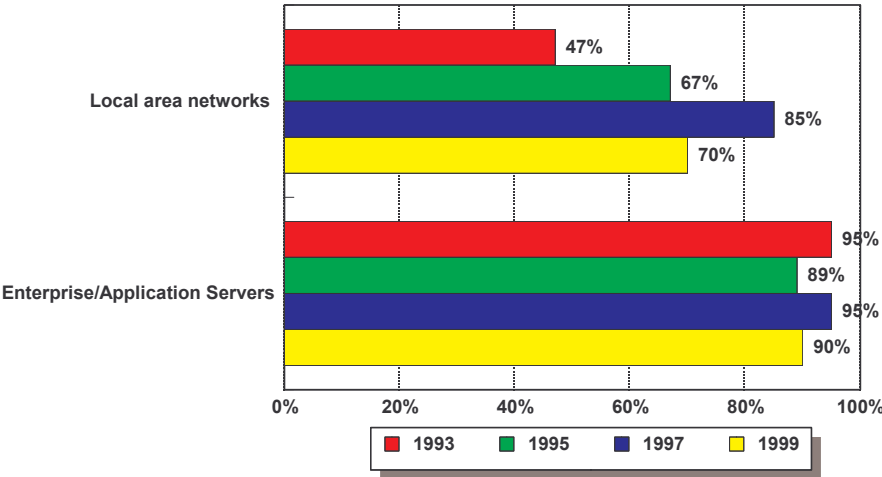
Systems Included In Business Continuity Programs *Among Those with Formal Programs*



The low proportion of companies that include wide area networks in their business continuity programs is possibly a reflection of two issues: a lower penetration of these systems across American industry as well as the rapid increase in the growth of these system over the past few years. Just as with local area networks, the number of companies that make efforts to include these systems in their formal plans should increase significantly over the next few years. While few than half of companies included local area networks in their

business continuity programs in 1993, 70 percent include these systems in their current business continuity programs.

Systems Included In Business Continuity Program*
Among Those with Formal Program

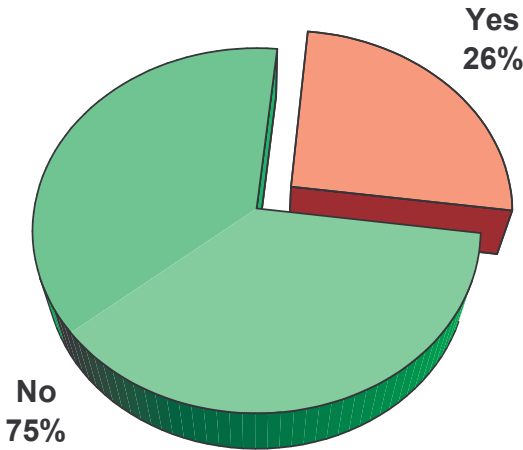


* Enterprise and application servers statistics from 1993 to 1995 are an average of “centralized mainframes” as well as “mainframe or midrange with distributed terminals”. Statistics from 1997 are based on “enterprise and application servers systems including mainframe and midrange systems.” Statistics from 1999 are based on “enterprise and application servers.”

One in four companies have experienced a disaster.

One in four (26%) of organizations participating in this survey have experienced a disruption of, or inability to access computer systems. Among these companies that experienced a disruption, 25 percent report having a disruption of more than 24 hours.

**Company Has Experienced Disruption
In Past Five Years**



The length of the disruption for the one in four organizations that experienced a disruption exceeded 24 hours. The median length of time of these companies' computer disruptions was eight hours.

Company Has Experienced Disruption

| Length of Disruption | Total |
|-----------------------------|---------|
| Four hours or less | 33% |
| Five to eight hours | 18% |
| Nine to 24 hours | 20% |
| More than 24 hours | 24% |
| Median Length of Disruption | 8 hours |

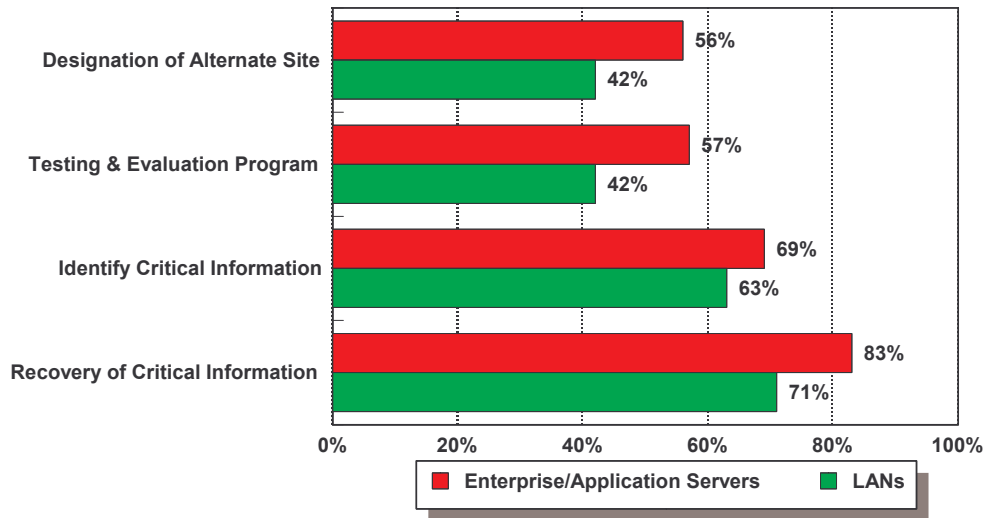
The ongoing high degree of work area vulnerability is a result of organizations continuing to ignore some of the most critical elements of business continuity planning.

Only slightly more than half of organizations with enterprise and application servers and about four in ten organizations with LANs have a written set of programs or requirements for the two most critical elements of a business continuity plan.

- Designation of alternative sites to relocate to in event of a disruption

- Having a testing and evaluation program for a recovery plan

Critical Procedures of Business Continuity Plan

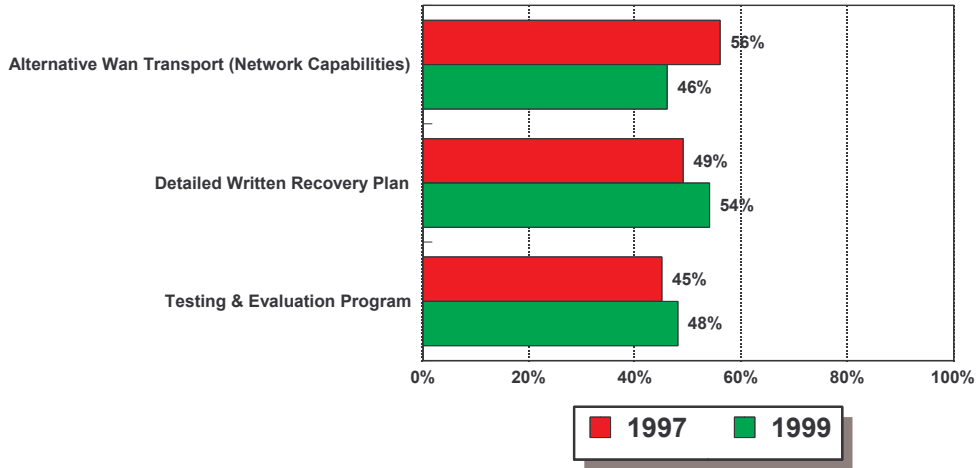


This is fundamentally unchanged since 1995 for both enterprise and application servers and for local area networks.

Two other critical aspects of this planning process for enterprise and application servers and for local area networks also remain unchanged. In 1997, a majority of those organizations with LANs had a written procedure in place for either the recovery (73%) or identification (59%) of critical information. Two years later, 71 percent of organizations with LANs have a written procedure for recovery of information and 63 percent have a written procedure for identifying this information.

Overall, only half (54%) of those companies with wide area networks have detailed written recovery plans in place. In addition, less than half of companies with wide area networks (46%) have taken efforts to provide alternative network capabilities as needed.

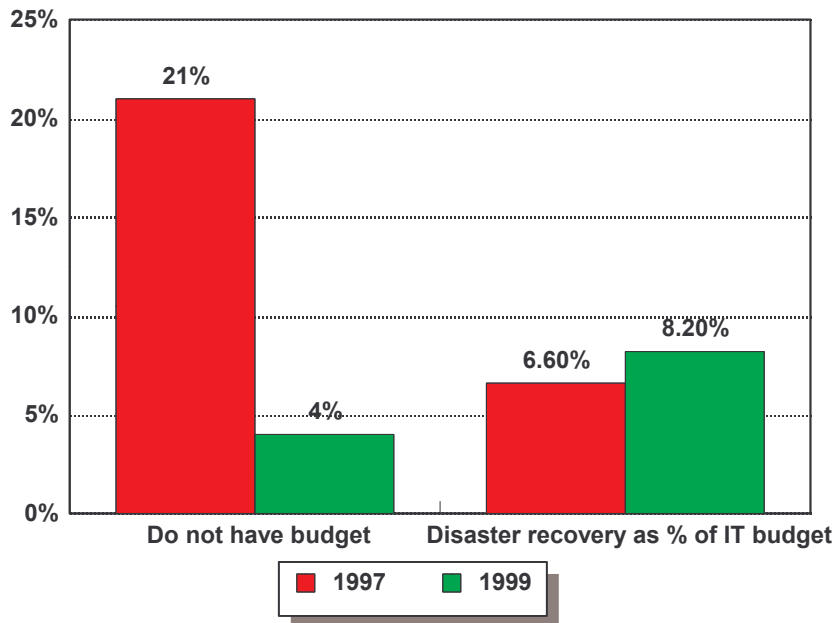
Critical Procedures of Business Continuity Plan *Wide Area Networks*



Companies have significantly increased their allocations for business continuity.

In 1997, 21 percent of companies did not have a budget for this function. Currently, only four percent of companies say they do not have a budget for business continuity. Accordingly the average business continuity budget has increased from, 6.6 percent of IT budgets to 8.2 percent today.

IT Budgets For Business Continuity

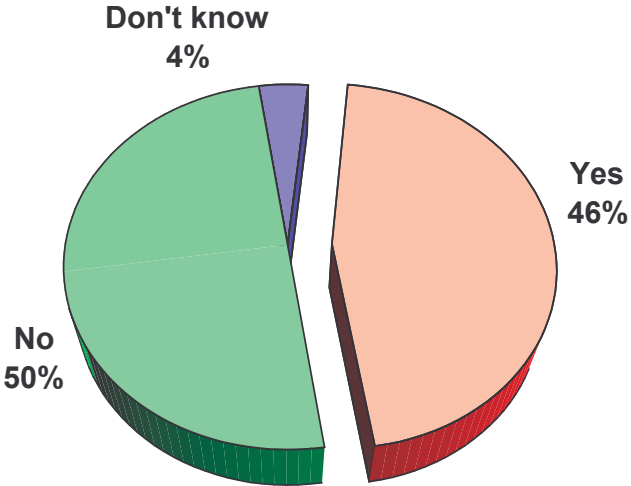


Benchmarking Business Continuity

Nearly half of the organizations surveyed require 99 percent or greater availability of applications.

Forty-six percent of companies' applications require applications to have 99 percent availability, yet few have the business continuity measures in place to ensure this level of availability.

Require 99% Or Greater Availability Of Applications



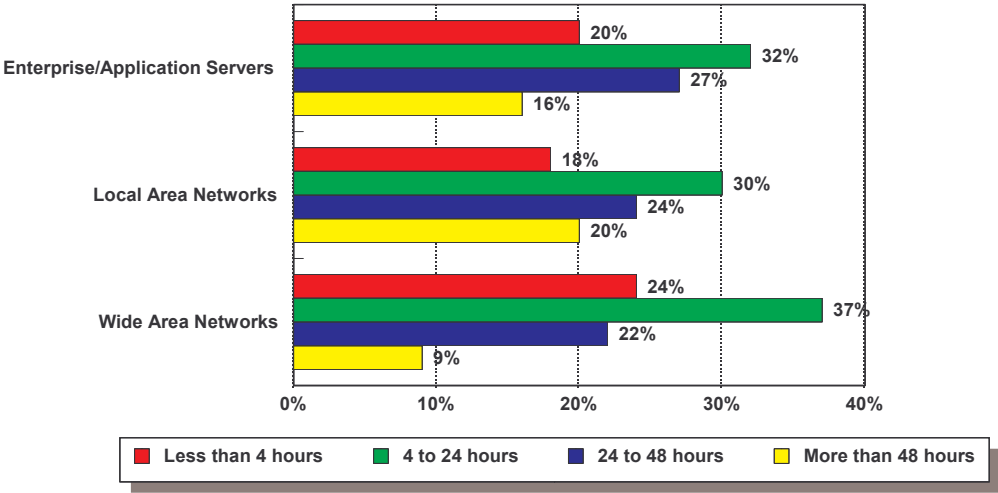
The actions taken to ensure this availability include:

- Fault tolerant hardware 66%
- Redundant hardware (on site) 56%
- Redundant hardware at Business Continuity site 32%
- Clustering (onsite) 27%
- Standby applications at Business Continuity site 21%
- Remote clustering 11%
- Don't take steps 13%

More companies set recovery time objectives than recovery point objectives

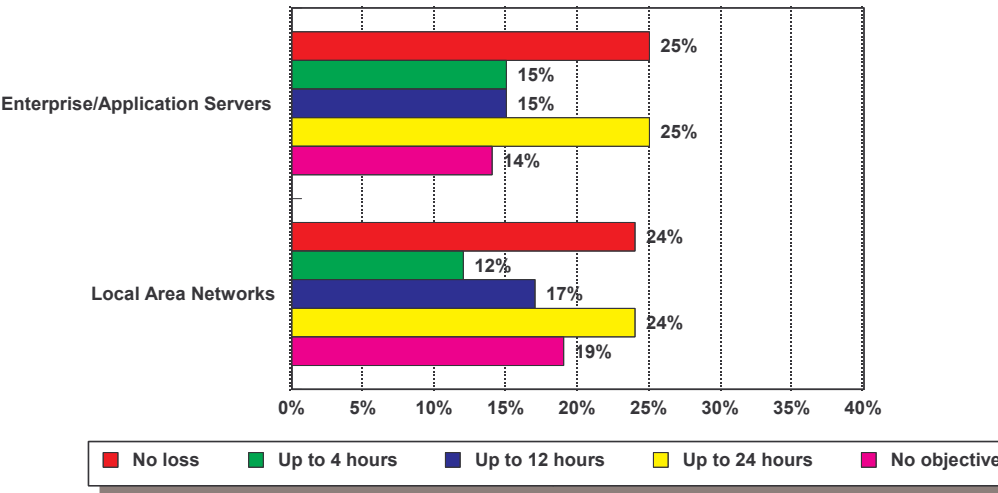
Companies typically look for a recovery time objective (downtime) of between four and 24 hours. One in five companies are even more rigorous, looking for a recovery time objective of less than four hours.

Recovery Time Objectives
Among Companies with Each Type Of System



They take a more stringent view in their recovery point objectives (point of data loss) with one in four companies saying they can tolerate no loss of data under these circumstances. Not surprisingly, those companies in financial services are much more likely to set rigorous standards in these areas.

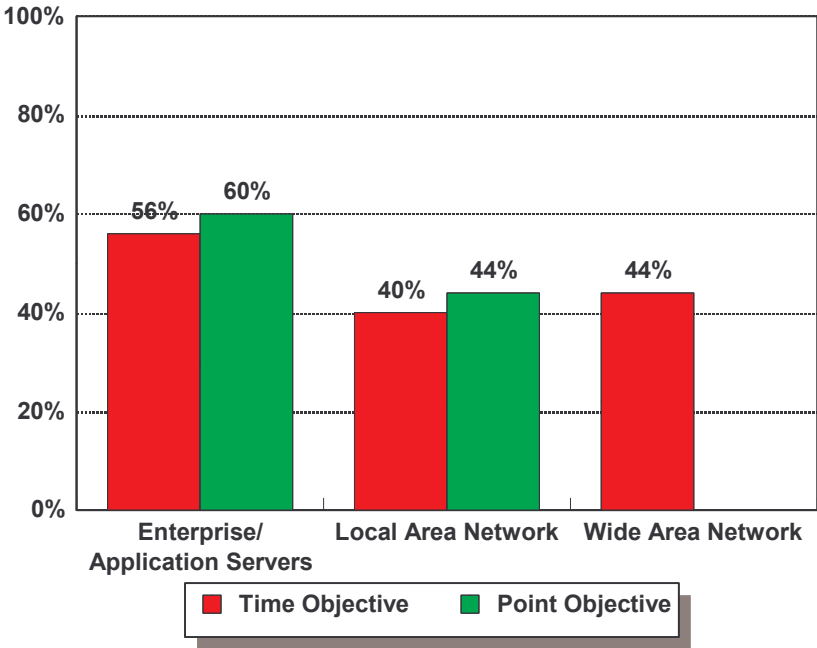
Recovery Point Objectives
Among Companies with Each Type Of System



Few companies have validated their recovery time and point objectives.

While many companies have set high standards for recovery time and point objectives, relatively few have taken the necessary precautions to make sure that these time and point objectives are properly validated. Just over half of those with enterprise or application servers have validated recovery time and point objectives for these systems and only about four in ten have taken the same precautions with their local area networks. Only 44 percent have validated recovery point objectives for their wide area networks.

Company Has Validated Objectives
Among Companies with Each Type Of System

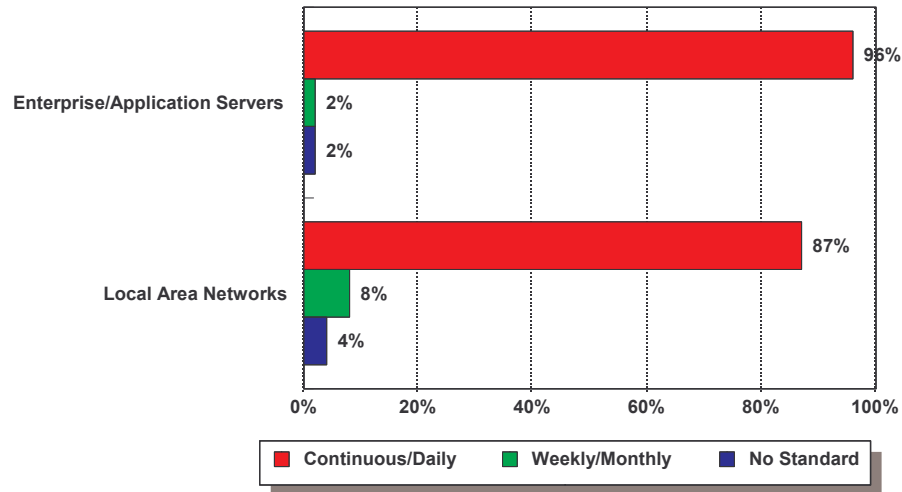


Backup and Data Storage Procedures

The vast majority of America's largest companies continue to follow rigorous data backup procedures.

In about nine out of ten instances the standard procedure is at least one daily backup of the data stored on the system. The frequency of following these standard backup procedures in enterprise and application servers remains unchanged since 1993.

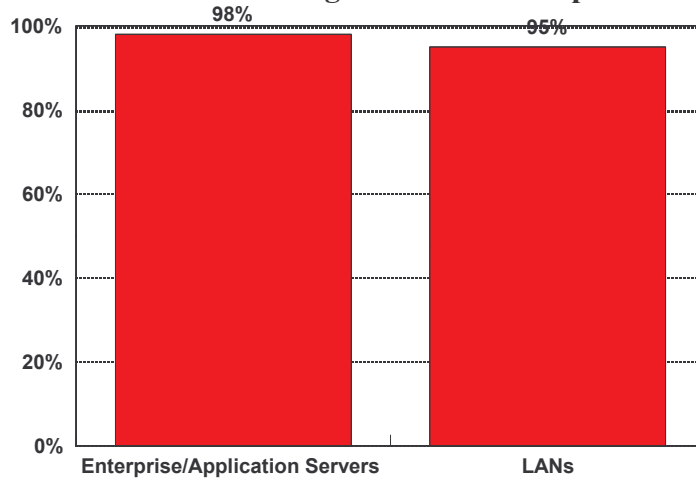
**Standard Procedures for Backing Up Data
Among Companies with Each Type Of System**



The frequency of backups for LANs, on the other hand has increased significantly. Today, seven in eight (87%) organizations use a continuous or daily backup as their standard backup procedures for their LANs. This compares to 74 percent in 1997. Overall, 96 percent of LAN users follow some standard backup procedure for their systems. This is a significant increase since 1993 when only 45 percent of organizations with LANs used a continuous or daily backup procedure.

In the vast majority of cases, organizations with backup procedures follow those protocols in almost all (*about 19 out of 20*) cases.

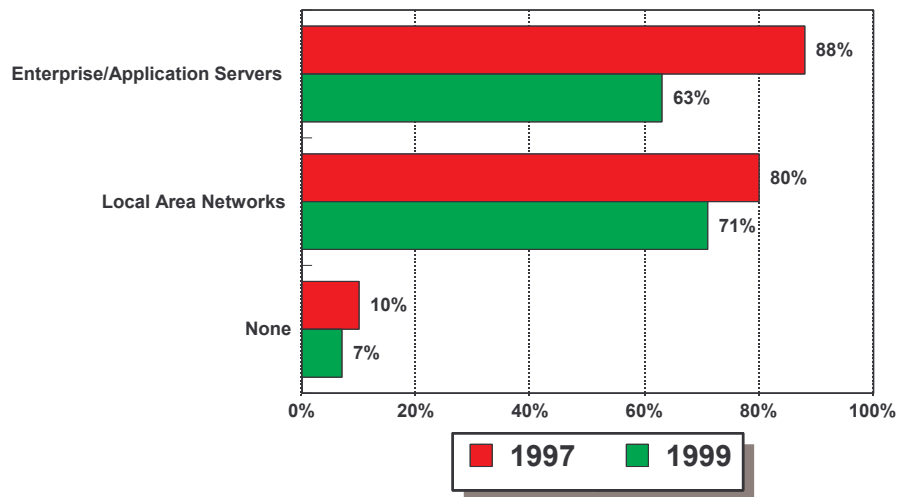
Likelihood Of Following Standard Backup Procedures



Less than two-thirds of companies use automated electronic backup systems.

Only 63 percent of companies are using these systems for their enterprise and application servers. Local area networks — *traditionally the most vulnerable corporate computing system* — are only somewhat more likely to be protected by these systems. Overall, 71 percent of LANs have automated electronic backups in place. This compares to 80 percent in 1997.

Use of Automated Electronic Backup Systems Among Companies With Each Type Of System



Profile of Respondents

Organization Profile

| | |
|--|---------------|
| <i>Primary Industry</i> | |
| Services | 33% |
| Manufacturing | 37% |
| Public Administration | 2% |
| Finance, Insurance and Real Estate | 8% |
| Wholesale/Retail Trade | 10% |
| | |
| <i>Average Annual Revenues</i> | \$809 million |
| | |
| <i>Average Number of Employees</i> | 6,245 |
| | |
| <i>Median Number of Full-Time Disaster Recovery Professionals</i> | 1 |
| | |
| <i>Percent of IT Budget Allocated for Business Continuity (average)</i> | 8.2% |

Executive Profile

| | |
|--|-----------|
| <i>Job Title</i> | |
| Executive | 48% |
| Manager/administrator | 35% |
| Data processing (<i>general</i>) | 6% |
| Engineer | 2% |
| | |
| <i>Job Responsibilities</i> | |
| Administration of computer and information systems | 97% |
| Determination of computer and information systems needs | 97% |
| Approval of computer and networking consultants | 86% |
| Approval or selection of manufacturers of computer and networking hardware and/or software | 92% |
| Responsibility for Business Continuity | 96% |
| | |
| <i>Average Time In Current Position</i> | 5.4 years |