BUSINESS CONTINUITY PLANNING: A COMPREHENSIVE APPROACH

Virginia Cerullo and Michael J. Cerullo

The risks of business interruption expand as companies become more dependent on information technology (IT) infrastructure. A comprehensive approach to business continuity planning seeks to mitigate against all major business interruptions of business systems. This article analyzes recent national and international surveys to develop insights about the current status of business continuity plans, including perceptions about internal and external information security threats.

EVERY COMPANY IS SUSCEPTIBLE TO natural disasters, such as earthquakes, hurricanes, and floods, which occur regularly throughout the world. The Federal Emergency Management Agency (FEMA) states that between 1976 and 2001, a total of 906 major disasters were declared in the United States.[1] Tens of thousands of organizations of all sizes were affected by these disasters. Unless firms prepare in advance, disasters inevitably shut down business operations. And the longer a firm's operations are shut down, the more likely it will never reopen for business. A study by Datapro Research Company found that 43 percent of companies hit by severe crises never reopen, and that another 29 percent fail within two years.[2] According to FEMA, of all the businesses damaged by Hurricane Andrew in 1992, 80 percent of those lacking a business continuity plan (BCP) failed within two years of the storm.

The potential causes of business interruption are not only from natural disasters, but are multifaceted, including interruptions caused by human error, utility disruptions (such as power outages), and malicious threats from outsiders. The risks of business interruption have therefore expanded as companies increasingly depend on information technology (IT) infrastructure and become more linked to external networks. The threat of cyberterrorism — including unauthorized access to a system, disruption or denial-of-service, unauthorized use of a system, or unauthorized changes to system hardware or software — can be as destructive as physical acts of terrorism. Quickly recovering from any type of business interruption, whether from a natural disaster or a telecommunication breakdown, is critical to a company's survival as a going concern.

Many companies have developed a disaster contingency recovery plan (DCRP). Although a DCRP is vital, it is primarily a reactive approach (i.e., a corrective control) and not a comprehensive plan for risk management. In contrast, a business continuity plan (BCP) seeks to eliminate or reduce the impact of a disaster condition *before* the condition occurs.

The Ernst & Young Global Information Security 2002 Survey revealed that critical busi-

VIRGINIA CERULLO and MICHAEL J. CERULLO are professors of accounting at Southwest Missouri State University in Springfield. Both authors are also CPAs and CFEs (Certified Fraud Examiners).

There is no single recommended plan for business continuity; instead, every organization needs to develop a comprehensive BCP based on its unique situation.

ness systems were increasingly interrupted: more than 75 percent of organizations worldwide experienced unexpected unavailability.[3] Thus, every firm needs a comprehensive BCP that addresses both internal and external threats.

BASIC COMPONENTS OF A BUSINESS CONTINUITY PLAN

A BCP is designed to avoid or mitigate risks; to reduce the impact of a crisis (i.e., disaster condition); and to reduce the time to restore conditions to a state of "business as usual." There is no single recommended plan for business continuity; instead, every organization needs to develop a comprehensive BCP based on its unique situation. A BCP should also be dynamic, evolving as the business environment changes and its dependency on advanced technology changes.

The business continuity planning process should address three interdependent objectives:

1. Identify major risks of business interruption.
2. Develop a plan to mitigate or reduce the impact of the identified risk.
3. Train employees and test the plan to ensure that it is effective.

The three basic components of a BCP to achieve these objectives are described below.[4]

Business Impact Analysis (BIA)

The business impact analysis (BIA) identifies critical functions the business must perform to stay in business (i.e., make money, provide mandated services); identifies risks to critical business functions and rates those risks according to probability of occurrence and impact on the business; recommends avoidance, mitigation, or absorption of the risk; and identifies ways to avoid or mitigate the risk.

In today's business environment, identifying risks has become a watchword. Recently, many leading firms have adopted an enterprise-wide risk assessment strategy and have established a framework, or database, of risks identified for their companies. Business continuity planners should be participants in any strategic risk assessment process and help establish a risk awareness environment.

Disaster Contingency Recovery Plan (DCRP)

Many companies have developed a disaster contingency recovery plan (DCRP), which specifies procedures to enact when a disaster occurs. It includes identification of primary and alternate team members and their specific duties, including executive management roles; notification procedures and alternate meeting site locations; work-around processes to keep the function operational while damaged resources are being restored to a "business as usual" condition; a contact list of all personnel and the functions they are qualified to perform; identification of all internal and external vendors and each vendor's primary and alternate contacts; and report forms (expenses, activities, etc.). A DCRP is therefore an integral part of a BCP.

Training and Testing

Training and testing includes developing a test methodology, simultaneous testing and training of the disaster recovery team, followed by BCP revision and simultaneous testing and training again. As a major component of the BCP, testing is essential to determine whether the BCP is adequate to address critical risks. In addition to ensuring that the disaster recovery team members — both primary and alternates — know what to do, testing under increasingly realistic conditions helps develop confidence and avoid panic during a disaster event.

Senior management backing of a BCP initiative ensures organizational commitment and adequate funding for business continuity planning. Yet even today, many executives view the BCP as a way to spend money with little, if any, return on the investment. Table 1 identifies some potentially useful Web resources for business continuity planning; some of these sites provide specific examples that may be useful to companies either developing or reevaluating their business continuity strategy. The detailed BCP outline developed by Paul Kirvan, published in the *Contingency Planning and Management* journal, is also a useful resource.[5]

Several recent surveys also provide some insight into the status of business continuity planning in companies throughout the world. The findings published in the Ernst & Young Global Information Security 2002 Survey,[6] based on responses from 459 CIOs and IT directors from medium- to large-sized companies worldwide, reveal that only 53 percent of these companies had a BCP. Of these companies with an in-place

TABLE 1 Leading Disaster Recovery and Business Continuity Web Sites

www.itaudit.org (Institute of Internal Auditors)
www.auditnet.org (AudioNet)
www.ContingencyPlanning.com (Contingency Planning & Management)
www.drj.com (Disaster Recovery Journal)
www.disasterrecoveryworld.com (Disaster Recovery World)
www.dlttape.com/proveit/steps/plan/test/ (Quantum Corp.)
www.wa.gov/DIS/CSD/drhopage.htm (Washington State Department of Information Services)
http://helpnet.ut.cc.va.us/NOC/Mainframe/drplan.htm (Virginia Community College Utility)
www.sun.com/storage/white-papers/backup-article2.html (Sun Microsystems)
www.labmice.net/disaster.htm (LabMice.Net)
www.state.mo.us/mo/samii/projinfo/implement/techbp/tech23.html (State of Missouri and American Management Systems)
www.state.me.us/bis/prod/Disaster.htm (State of Maine)
www.comdisco.com (Comdisco Inc.)
www.hp.com/go/recovery (Hewlett-Packard)
www.gedisasterrecovery.com (GE Capital Information Technology Solutions)
www.ibm.com/services/continuity (IBM Corp.)
www.sungardresponse.com (SunGard Recovery Services LP)
www.dri.ca (Disaster Recovery Institute Canada)
www.drie.org (Disaster Recovery Information Exchange)

Modi ed from: Michael Barrier. "Preparing for the Worst," *Internal Auditor,* December 2001, p. 60.

BCP, many had also not gone through the expected activities to develop a comprehensive plan. For example, more than 40 percent of the companies claiming to have a BCP had not carried out a business impact analysis (BIA) and prioritized their critical business processes. In addition, 21 percent of the survey respondents had not tested their plans and less than 50 percent of the responding firms had not established recovery timelines with the business, which could mean a wide expectation gap between what the business needs and what the plan provides for.[7]

A survey of business continuity planning professionals conducted in mid-2002 revealed that 38 percent of the 855 responding companies had activated their BCPs (CPM and Strohl Survey, 2002). This has led Brian Turley, President of Strohl Systems, to conclude that:

> "It is no longer a matter of 'if' you have to activate your plan, but 'when' you will have to activate your plan."[8]

> "Managers of a company may be morally and ethically bound to make decisions and plans that will ensure that the business continues to operate."[9]

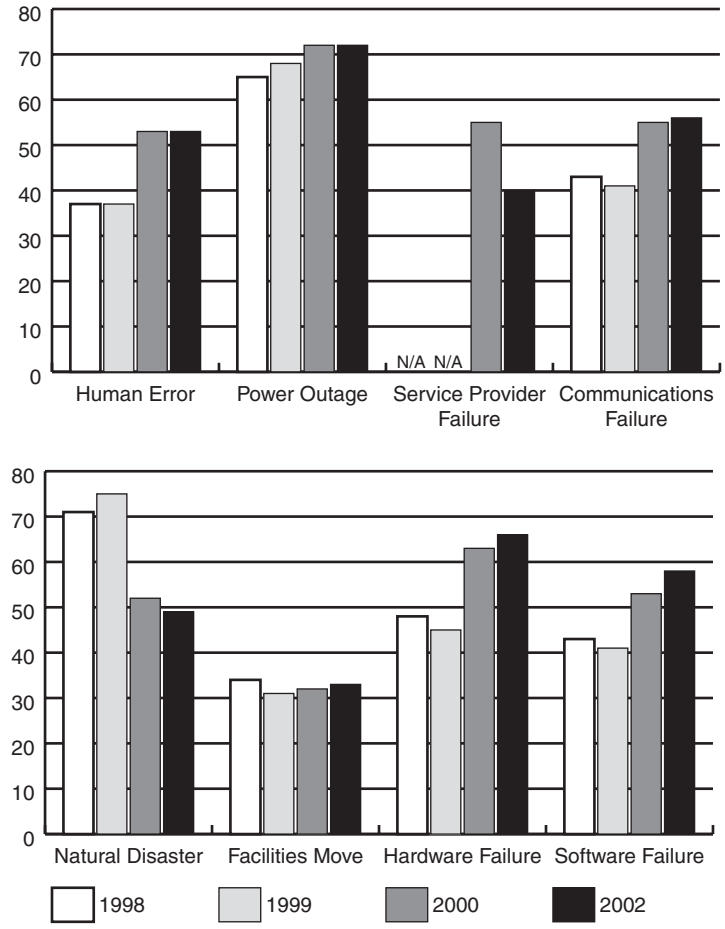
The next section provides a review of recent empirical data concerning the internal and external causes of business interruptions. For those with in-place BCPs, these survey findings on actual and potential causes of business interruptions can be used to help direct management attention to areas of a BCP that need enhancement.

INTERNAL AND EXTERNAL CAUSES OF BUSINESS INTERRUPTIONS

The CPM and Strohl Survey 2002 found that 50 percent of the responding continuity planning professionals were most concerned with accidental failures (i.e., internal causes, such as power outages, equipment failures, software errors, and operational errors). The threat of natural disasters (i.e., earthquakes, floods, and hurricanes) ranked as the second-greatest cause of concern with 29 percent. Intentional externally caused disasters (i.e., such as hackers, terrorism, acts of war) ranked third with 21 percent.[10]

The existence of multiple causes of business interruptions is also documented in the Business Continuity Benchmark survey results published by CPM/KPMG in 2002.[11] Based on 624 respondents, the results shown in Figure 1 provide comparisons over four years for business interruptions due to both internal and external causes: human error, power outage, service provider failure, communications failure, natural disaster, facilities moves, hardware failure, and

FIGURE 1 Business Interruption Risk (*Source:* CPM/KPMG Business Continuity Benchmark Survey, Witter Publishing Corp., 2002.)



software failure. It is interesting that the only actual or perceived risk that *decreased* between 1999 and 2002 was the risk from natural disasters. Although natural disasters were still a significant threat, the recent survey respondents, who included contingency planners, identified power outages, hardware and software failures, and communications failures as more common business interruption risks.

The Ernst & Young 2003 Survey also reveals a heightened recognition of *information security* threats. The threat to information security perceived as the highest intensity (recognized by 77 percent of respondents) was a major virus or worm. However, employee misconduct with information systems was rated next highest (by 57 percent of respondents).[12] These two types of attack or abuse were also listed the highest in the 2003 CSI/FBI Survey based on reported incidents.

Taken together, these surveys provide clear evidence that companies now appear to consider internal causes of business interruption to be multifaceted, from operational disruptions due to human error, to technical disruptions due to hardware and software failures. However, companies must recognize that to prevent business interruption, it is necessary to address all the complexities of internal operations to support their business, as well as a wide range of external causes of business interruption.

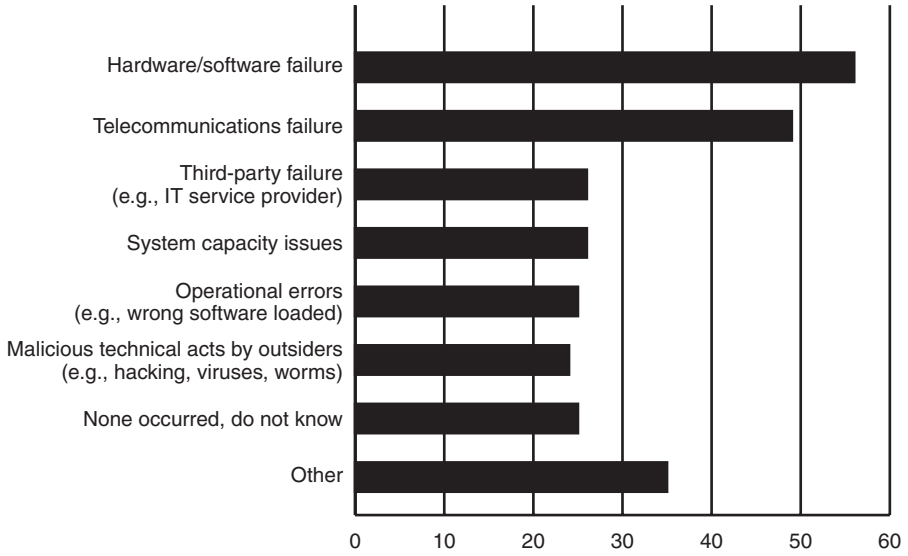
Below we discuss additional survey results for internal causes and external causes separately.

Internal Causes

Understanding the key internal causes of business interruptions will assist firms in enhancing their BCPs. The traditional focus for BCPs has been the impact of hardware or software failure on maintaining and processing critical data. Clearly, this continues to be a major concern. As seen in Figure 2, the top two causes for the unavailability of critical business systems cited in the Ernst & Young Survey 2002 were hardware or software failure (56 percent) and telecommunications failure (49 percent).[13] However, Figure 2 also reveals that a high number of failures were due to system capacity issues and operational errors. These internal causes of failure could be the result of poor management of operational basics, such as sound operational procedures for loading new software, change management, and capacity planning.

Further, the possibility of an internal attack on systems is often overlooked or underemphasized. Only 41 percent of the organizations included in the Ernst & Young Survey 2002 expressed concern about the potential for internal attacks on systems, despite overwhelming evidence of the high number of these attacks.[14] In another 2002 report, Vista Research estimated that 70 percent of security breaches — causing losses of more than $100,000 — were perpetrated internally, often by disgruntled employees.[15] The 2003 CSI/FBI Computer Crime and Security Survey reports insider abuse of network access as only slightly below virus attacks as the most cited form of attack or abuse.[16] In addition, although virus and worm attacks are discussed under "external causes" (see below), these attacks could originate internally.

FIGURE 2 Causes for Unavailability of Critical Business Systems (*Source:* Ernst & Young, Global Information Security Survey, 2002.)



The Ernst & Young Survey 2003 found that senior managers still focus more on the publicized external attacks than potential internal attacks. As shown in Figure 3, when respondents were asked to rate the relative intensity of threats expected over the next 12 months, employee misconduct with information systems was rated as a much lower threat than a major virus or worm.

External Causes

In the 1980s and early 1990s, many firms established a DCRP primarily to address natural disasters. In fact, many waited until a natural disaster actually occurred to their company before developing a DCRP. Unfortunately, too few firms have updated their business continuity strategy to recognize man-made external threats. A major challenge today is to manage the growing threat from these external risks due to recent changes in the IT environment. As seen in Figure 3, for example, the highest threat perceived over the next 12 months was a major virus or worm attack.

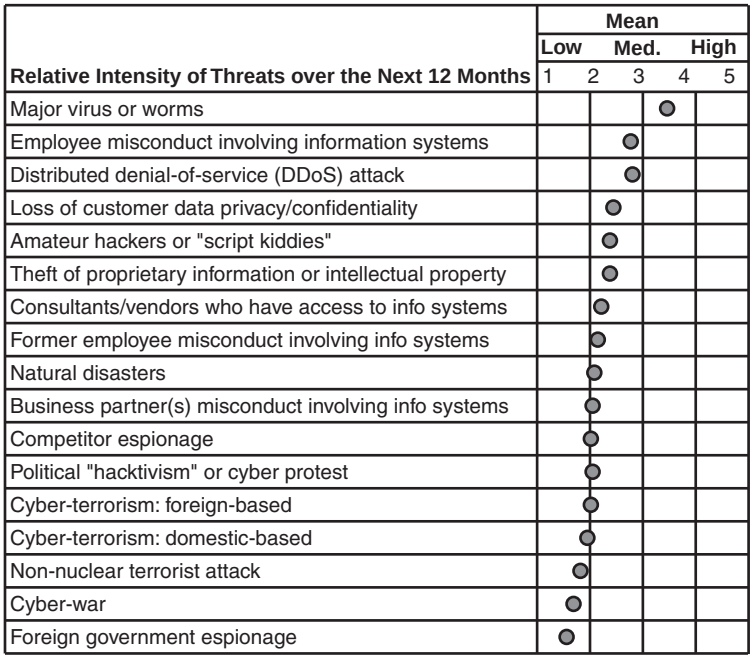
Based on responses from 530 computer security practitioners in U.S. corporations and government agencies, the findings of the 2003 CSI/FBI Computer Crime and Security Survey reveal that 56 percent of respondents reported that unauthorized use and theft of proprietary information caused the greatest financial loss ($70,195,900). The second-most expensive computer crime among survey respondents was denial-of-service ($65,643,000). Although not the most expensive, virus incidents were the most frequently cited forms of attack.[17]

The BCB 2002 Survey, designed after the 9/11 terrorist attack in the United States, added a question to determine the extent to which companies had been affected by, or at risk of, threats of (1) information security breaches and (2) terrorist activities. More than two thirds of companies surveyed still did not regard either malicious activity as a threat to their company. While it may be understandable that companies could not imagine an event similar to those of 9/11 happening to their company, it is surprising that less than a third of the companies did not perceive at that time a threat from an information security breach. In contrast, the disaster recovery coordinator at the Johns Hopkins Hospital, Bill Rider, has commented:

> "While we continue to be at risk of physical terrorist attacks, I think the risk of an electronic terrorist attack via denials of service, worms, etc. is becoming much greater, given our ever-growing dependence on the electronic infrastructure."[18]

The Information Security Surveys conducted by Ernst & Young over three years (2001, 2002, and 2003) provide some additional insight into managers' perceptions of these security risks and their firms' capabilities to manage

FIGURE 3 Perceptions of Threat Levels 2003 (*Source:* Ernst & Young, Global Information Security Survey, 2003.)



them. In the Ernst & Young Survey 2001, security breaches by external parties were the biggest concern, inhibiting development of E-commerce for 66 percent of respondents; only 33 percent of respondents were confident that they could detect a hacking attack.[19] In the Ernst & Young Survey 2002, a somewhat higher 40 percent were confident they would detect a systems attack, but another 40 percent of responding firms did not even investigate information security incidents.[20] In the 2003 survey, 90 percent of respondents said that information security was of high importance for achieving their overall objectives. However, more than 34 percent still rated their organizations as less than adequate in their ability to determine whether their systems are currently under attack, and more than 33 percent of respondents reported an inadequate capability to respond to information security incidents.[21]

While external disasters have the potential for unlimited destruction, the damage from viruses and other computer threats can often be quantified. For example, Computer Economics (Carlsbad, California) estimates that corporations spent more than $12 billion in 2001 to clean up virus damage. The Code Red virus alone was estimated to have caused $2.6 billion in damages and infected 300,000 computers.[22]

Benny D. Taylor (Disaster Recovery Institute International) predicted in early 2002 that an increased dependence on E-business would also increase the need for spending on disaster recovery to reduce the risk of short-term interruptions; he estimated these costs to be from an average of 3 percent to 7 percent of data center budgets. Published estimates of the costs of systems downtime for company Web sites include the following:[23]

- Downtime is costing major Internet players an estimated $8000 per hour (Forrester Research).
- Downtime costs $1400 per minute on average (Oracle).
- Typical medium-sized business downtime costs average $78,000 per hour; these sites typically lose more than $1 million annually due to downtime (see Table 2) (IDC).

These types of published costs emphasize the importance of identifying business environments that are increasingly exposed to external IT-related risks; an example of a questionnaire to assist in identifying these technology risks to corporations can be found online at the ContingencyPlanning.com Web site.[24] Every year, the list of sophisticated external threats to IT environments becomes longer. Therefore, informa-

TABLE 2 Average Hourly Effect on Businesses of Web Site Downtime

Type of Business	Average Hourly Impact
Retail brokerage	$6,450,000
Credit card sales authorization	$2,600,000
Home shopping channels	$113,750
Airline reservations centers	$ 89,500
Package shipping service	$ 28,250

tion security must be considered a critical aspect of a comprehensive BCP.

INTEGRATING BCP AND IT SECURITY PLANS

As discussed, information security threats include both internal and external risks of business continuity. As firms become more dependent on IT, there is an increased need to integrate business continuity planning with IT security planning.

Many companies have included both BCP and security measures as a part of their IT budget. The Ernst & Young Survey 2002 found that only 29 percent of responding firms treated BCPs as a business unit expenditure, and 45 percent said it was within the IT budget. These percentages indicate that too many firms still perceive business continuity as the responsibility of the IT function alone. Instead of addressing the multifaceted risks to business continuity, these firms appear to remain focused on traditional recovery of hardware and software.[25]

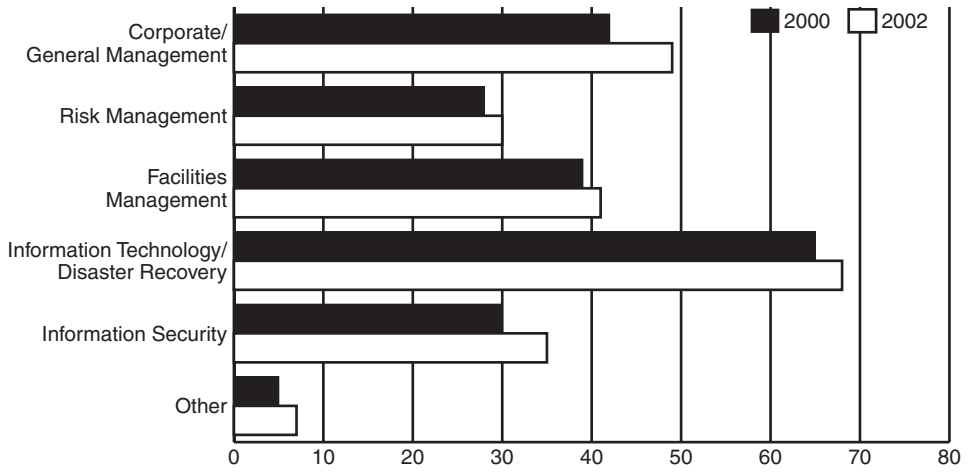
However, the BCB Survey 2002 shows an encouraging trend (see Figure 4): BCP is integrated with several functions. Although about 45 percent considered IT as the primary owner, approximately 35 percent of respondents cited corporate/general management as the primary owner of the business continuity programs.[26]

The results of a 2003 CPM readership survey also indicated a clear relationship between BCP and information security: 70 percent of respondents indicated that IT security was very important to the overall business/contingency planning process. However, the exact terms of the relationship between BCP and information security remain unclear: 13 percent of the business continuity/contingency planners stated that they had total responsibility for IT security, 29 percent had significant responsibility for IT security, and 43 percent said they had peripheral responsibility for IT security.[27]

Rich Corcoran, Eastman Kodak's manager of business recovery and information systems, predicts that:

> "Over the next three years, I see the main focus of the BCP driven out of [IT] and placed in a corporate position. This will be true for the largest banking and financial institutions, with some creep into large manufacturing corporations. Clearly, a well-designed BCP will be deeply integrated into the business units and business function."

FIGURE 4 Integration of the BCP (*Source:* 2002 CPM/KPMG Business Continuity Benchmark Survey, Witter Publishing Corporation, 2002.)



New technology can make testing easier; and perhaps in ten years, intelligent BCP software will be available to automatically update and maintain plans.

However, Corcoran also predicts that the BCP for small and medium-sized companies will continue to be closely aligned with IT.[28]

To ensure that the BCP is corporatewide, a high-level staff position that is independent of IT or other existing organizational functions might need to be created. For example, managers might wish to follow the lead of some companies that have established the position of "Chief Continuity Officer."

TESTING THE BCP

As described, Training and Testing is a major BCP component; it is essential that a BCP be thoroughly tested and that employees be trained. Evidence abounds concerning the number of IT-dependent companies, without tested BCPs, that have failed to survive a disaster. BCP testing will provide the firm with the assurance that all necessary steps are included in the plan.

However, recent surveys reveal that too many firms are ignoring or minimizing the importance of the Testing component as part of the development of a comprehensive BCP. In a 2001 survey by Ernst & Young, only one third of the responding companies claimed to have tested their plans.[29] The E&Y 2002 Survey reports a much higher percentage of firms testing their plans: only 21 percent reported that they had *not* tested their BCP.[30] Similarly, the CPM and Strohl 2002 survey found that 60 percent of respondents tested their plans either yearly (37 percent) or every six months (23 percent); only 10 percent did not test their plans at all.

The CPM and Strohl 2002[31] survey also provides additional insights into the different types of BCP testing with different levels of intensity (a breakdown on the type and level of testing was not provided in the other studies):

- 15 percent performed only IT-specific tests
- 8 percent performed tabletop walk-throughs
- 8 percent performed call list tests, business unit tests, or enterprisewide, full-scale tests
- 58 percent used a combination of these methods

New technology can make testing easier; and perhaps in ten years, intelligent BCP software will be available to automatically update and maintain plans. In the meantime, firms must evaluate their testing procedures to ensure that they are practical, cost-effective, and appropriate. Thorough testing will ensure a high level of confidence and recovery capability.

CONCLUSION

Recent surveys indicate that the majority of firms recognize natural disasters as a significant threat and may have an in-place disaster contingency and recovery plan (DCRP). However, such DCRPs only address one class of threats, while ignoring other serious threats, both internal and external. This article provides guidelines for developing and improving a firm's business continuity plan (BCP), which has three components: (1) a business impact analysis that takes into account a wide variety of potentially serious internal and external threats, (2) a DCRP, and (3) a training and testing component. A large number of firms are minimizing the importance of testing and maintaining the BCP, yet testing is critical to developing an effective BCP and to assess the effectiveness of the BCP before an actual disaster occurs.

There is clear evidence that a company without a BCP has a low probability of survival. However, even after the 9/11 terrorist attacks in the United States, only 53 percent of the firms surveyed in 2002 by Ernst & Young had a BCP. Further, based on an analysis of data reported in several major published surveys, many of the existing BCPs are seriously deficient and outdated, as they do not address many of today's major risks of business systems interruption. The overwhelming conclusion is that firms must periodically reevaluate the comprehensiveness of their business continuity strategy to avoid catastrophic consequences from a wide variety of serious internal and external threats, including increasing information security threats.

Current trends are to transfer the primary ownership of the BCP to corporate or general management and to integrate business continuity and IT security planning. Some companies have given this responsibility to a new corporate position, a Chief Continuity Officer. While no amount of security measures can provide absolute protection from all potential intrusions and disasters, a comprehensive BCP will dramatically increase a company's defenses and reduce the impact of any business interruptions. ▲

Notes

1. http://www.ferma.gov/library/lib01.htm.
2. Jan H. Schut. "Insurance: Lessons from Disasters," *Institutional Investor,* October 1990, p. 297.
3. Ernst & Young LLP. Global Information Security Survey, 2002, p. i.

4. The basic components are modified from: Glenn, John. "BCP 103: Business Continuity Defined," www.ContingencyPlanning.com/article_index.cfm?article=380.
5. Kirvan, Paul. "Essential Ingredients of a BC Plan," *Continuity Planning & Management,* April 2003, pp. 16–17.
6. Ernst & Young LLP. Global Information Security Survey 2002.
7. Ernst & Young, 2002, p. 11.
8. "Study Reports on Plan Activation, Testing," *Contingency Planning & Management* (September/October 2002), Vol. VII, No. 6, p. 12.
9. Emergency Response Planning, http://www.erplan.com/index2.htm.
10. "Study Reports on Plan Activation, Testing," *Contingency Planning & Management* (Sept./Oct. 2002), p. 12.
11. Hagg, Andy. "Benchmark Report: BCP in 2002," *Contingency Planning & Management* (July/August 2002), p. 8.
12. Ernst & Young, 2003, p. 7.
13. Ernst & Young, 2002, p. 11
14. Ibid, p. 8.
15. Cited in *The Economist*, October 24, 2002, "The Weakest Link."
16. 2003 CSI/FBI Computer Crime and Security Survey, p. 4.
17. 2003 CSI/FBI Computer Crime and Security Survey, pp. 3–4.
18. Ernst & Young, 2002., p. 3
19. Ernst & Young, 2001, p. 6.
20. Ernst & Young, 2002, pp. 7–8.
21. Ernst & Young, Global Information Security Survey 2003 (Issues at a Glance).
22. Carl Herberger, "Integrating Business Continuity and Information Systems," www.ContingencyPlanning.com.
23. Benny D. Taylor. "Evaluating and Selecting the Most Appropriate Continuity Strategy for Your Organization," Disaster Recovery Institute International, February 2002.
24. Anthony Scrimenti. "Corporate Technology Risk Assessment: A Questionnaire," www.ContingencyPlanning.com/article_index.cfm?article=422.
25. Ernst & Young, 2002, p. 3.
26. Hagg, Andy, p. 9.
27. Matt Migliore. "Business Continuity and Information Security," *Contingency Planning & Management*, July/August 2003, pp. 26–27.
28. Ibid.
29. Ernst & Young, 2001, p. i.
30. Ernst & Young, 2002, p. 11.
31. "Study Reports on Plan Activation, Testing," *Contingency Planning & Management,* Sept./Oct. 2002, p. 12.