A Five-Step Business Continuity Plan for CEOs
by Gary Lynch and Karen Avery

9/24/2002
Few companies were braced for the terrorist actions of September 11, 2001. Networks housing vital customer and financial data were severed without any secondary systems to take up the slack. Telecommunications connections were silenced. Supply chains were broken by the transportation gridlock. In all, according to Lloyd’s of London, as much as $10 billion in corporate losses from the World Trade Center attack was related directly to business interruption.

In some ways, the lack of preparedness was not surprising — after all, the unthinkable occurred that day. But what is remarkable is that the events of September 11 apparently have done little over the past year to heighten many chief executives’ concerns about their company’s business continuity — short-term or long-term — in the face of disruption, let alone disaster. In a Booz Allen Hamilton and Roper ASW survey of Fortune 1000 chief executives conducted two months after last year’s terrorist actions, fewer than half said they were evaluating alternative plans for business continuity to protect against an unexpected break in their distribution channels. Overall, the data suggested that CEOs were generally satisfied with their organization’s ability to respond to security threats, to handle disruptions to their business, and to support their relationships with business partners.

That sentiment is beginning to change. With regulators and insurers pressing ahead with policies forcing companies to take more aggressive action to protect themselves, their customers, their shareholders, and their communities, senior executives are placing renewed emphasis on business continuity planning as well as on building enterprise resilience. Business continuity planning aims to prevent or minimize damage from disruptions in operations. “Enterprise resilience” is Booz Allen Hamilton’s term for the integrated management of a company’s risk exposures wherever they might exist, whether in operations, technology, or even the business model itself.

Raising the Stakes

There are many reasons executives shy away from taking on a comprehensive overhaul of their company’s management of security risks. Some are concerned that it will be too expensive to tackle; others feel it’s too complex and overwhelming to fully understand; and many CEOs think that such an undertaking is nothing more than a technology issue and delegate it to IT departments. Such attitudes prevent companies from looking at the organization as a whole, a mistake because business continuity affects virtually every aspect of a company’s operations.

But the terrorist actions, as well
as pervasive cyber attacks, to which companies are always susceptible, have raised the visibility and escalated the discussions of business continuity. And as more examples come to light of companies routinely being threatened by IT systems disruptions or service denials — perhaps because of hackers, poorly designed networks, or the lack of planning to safeguard the most critical elements which is out for public comment, covers the actions that key banking, brokerage, and consumer finance companies need to take to bolster their ability to resume critical business activities in the event of future wide-scale disruptions. As company boards demand greater accountability from chief executives after the debacles at Enron, WorldCom, Qwest, and others, CEOs, under

“CEOs, under the gun to better control corporate financial activities, will increasingly be held responsible for risk management. These trends will be the dominant drivers of business continuity programs.”

of the organization — it’s likely that chief executives will begin to view the matter as less of an aberration and pay more attention to it.

Actually, they may have no choice. Increasingly, insurers are beginning to require that companies increase investment in protection against disruptions before they will offer coverage for losses. Regulators overseeing critical industries closely tied to the welfare of the economy and consumers, such as financial services, are taking the same stance. In August, the Board of Governors of the Federal Reserve, the Securities and Exchange Commission, the Office of the Comptroller of the Currency, and the New York State Banking Department issued a joint draft white paper covering ways to strengthen the resilience of the U.S. economic system. This report, the gun to better control corporate financial activities, will also increasingly be held responsible for risk management. These trends, we believe, will be the dominant drivers of business continuity programs during the next several years.

A Five-Step Plan
Fortunately, improving an organization’s management of risk exposures across the business, and strengthening its responses to threats and real attacks, does not have to be overwhelming. Indeed, preparation of a strong risk management program can be broken down into five steps:

Step 1: Design a business continuity plan. A company can begin by conducting a thorough business impact analysis to identify which organizational processes, products,
locations, lines of business, and
departments should be highlighted
in the continuity plan. Ideal recov-
ery times for incidents should also
be documented. This analysis
should generate a comprehensive
list of resource needs in the face of a
serious disruption — including per-
sonnel, computer hardware, net-
works, applications, communications
technology, specialized equip-
ment, office space at alternative
sites, equipment, and supplies. It is
also important that there be a sched-
ule for reviewing, and, if necessary,
updating the business continuity
plan on a regular basis.

**Step 2: Test the plan.** The best
to do this is to use the continu-
ity plan as a response playbook dur-
ing pre-scripted “war-game” exercis-
es. These should be conducted peri-
dically to ensure that new events
and conditions are not beyond the
scope of existing recovery proce-
dures. Taken as a whole, these ses-
sions, which precede hands-on test-
ing of the plan, should provide an
unbiased evaluation of how well the
business continuity plan would pro-
tect essential locations, business
processes, people, and technology.
After conducting the exercises,
management should identify ways
to improve the plan.

**Step 3: Develop a business conti-
nuity management infrastruc-
ture.** This infrastructure serves as a
command center and coordinates
reporting, response, transportation,
external communications, e-mail,
facilities, legal actions, loss control,
and resources during and after a cri-

gis or disaster. Essentially, it’s the
internal organization that adminis-
ters the business continuity plan. It
is critical to success to have a list of
assignments that shows who is
responsible — from CEO to legal
counsel to facilities staff — for
which resources and response activi-
ties during an incident. What is
equally important, but often over-
looked, is that there should be
guidelines for quick, accurate, and
appropriate notification of third
parties, such as media, shareholders,
police, regulators, and public utili-
ties. Just by creating this infrastruc-
ture, and linking it to the business
continuity plan, top management
can become more aware of their
organization’s vulnerability. For
example, they can see how frequent-
ly their companies actually suffer
potentially serious disruptions, a
measure that is difficult to obtain
without an infrastructure. (After
implementing an incident manage-
ment infrastructure, one insurance
giant recently found that in a six-

month period it faced 29 major
interruptions and more than 300
minor outages.)

**Step 4: Train employees in crisis
management.** There should be a
formal, written plan that educates
employees responsible for contin-
uity planning and crisis or incident
management. A series of mandatory
classes with a curriculum that mir-
rors the company’s business conti-
nuity plan is the best way to ensure
that employees are taught practical
knowledge that will fit with the
internal procedures to deal with dis-
ruption. In addition, the company’s
business continuity specialists — for
instance, those who led the creation
of the business continuity plan in
the first place — should remain in
touch with industry crisis manage-
ment best practices by being active
in such groups as the Contingency
Planning Exchange (www.cpe-

**“Enterprise resilience is Booz
Allen Hamilton’s term for the
integrated management of a
company’s risk exposures,
whether in operations,
technology, or even the
business model itself.”**
management infrastructure are effectively guarding the organization from natural disasters as well as cyber or physical attacks. For instance, all new technology initiatives need to be analyzed to show how system downtime would affect the business; this will help to determine how much redundancy (in the form of backup systems) is needed, and where. Benchmarking should be done to set goals for how well the company must perform during an actual incident — whether it is a virus, bad weather, an earthquake, a terrorist attack, etc. Among the possible guidelines: Recovery time should vary no more than 10 percent from the targets laid out in the continuity program; event assessment, reporting, and action plans must be prepared within 48 hours of an incident; and the company’s incident response and alert center should be activated within two hours of awareness of a threat. Other metrics might be used to evaluate whether employees have a basic understanding of crisis management policies and procedures, and whether they have done a sufficient number of disaster drills.

**Triumph of the Long View**

If structured correctly, an organization’s business continuity program should give it a flexible and focused framework for addressing multiple risks and security issues simultaneously in a way that involves all critical business units in designing and executing the plan. The resulting approach will promote cooperation across all significant technology and non-technology functions in the corporation, which is vital but a difficult management challenge for most companies.

As with all ambitious efforts atop the corporate agenda, a business continuity plan must have strong support from the chief executive; there must be a clear commitment to never let disruptions seriously hurt a company’s performance. Short-term thinking is often the reason this backing is missing — in other words, the CEO is simply not willing to sanction the expenditure of the money, time, and management resources necessary to make business continuity a core strategic objective and operating principle. When a crisis occurs, though — and serious vulnerabilities are suddenly uncovered — the result for companies can end up being much more costly long-term pain.

“A business continuity plan must have strong support from the chief executive; there must be a clear commitment to never let disruptions seriously hurt a company’s performance.”

**Related Articles**

“Security Concerns Prominent on CEO Agenda,” by Mark Gerencser and DeAnne Aguirre, s+b enews, 02/12/02. www.strategy-business.com/enewsarticle/?art=254087


strategy+business magazine
is published by Booz Allen Hamilton.
To subscribe, visit www.strategy-business.com
or call 1-877-829-9108