strategy+business enews

A Five-Step Business Continuity Plan for CEOs

by Gary Lynch and Karen Avery

9/24/2002

exclusive added-value from strategy+business

A Five-Step Business Continuity Plan for CEOs

Straightforward planning makes business continuity less of a mystery and management burden, and more of a strategic priority and opportunity.

by Gary Lynch and Karen Avery

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 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, 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 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.

> "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."

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,

Gary Lynch
(lynch_gary@bah.com) is a Booz Allen Hamilton vice president in New York, responsible for the Commercial Information Assurance and Business Resilience practice. With over 20 years of experience as a business and IT professional, he works with senior corporate executives to help manage operational risk, specifically in the area of business continuity and information security.

Karen Avery
(avery_karen@bah.com), a principal at Booz Allen Hamilton based in New York, is responsible for commercial information assurance solutions. Formerly, she was the chief information security officer at GE Capital.

locations, lines of business, and departments should be highlighted in the continuity plan. Ideal recovery 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 personnel, computer hardware, networks, applications, communications technology, specialized equipment, office space at alternative sites, equipment, and supplies. It is also important that there be a schedule for reviewing, and, if necessary, updating the business continuity plan on a regular basis.

Step 2: Test the plan. The best way to do this is to use the continuity plan as a response playbook during pre-scripted "war-game" exercises. These should be conducted periodically to ensure that new events and conditions are not beyond the scope of existing recovery procedures. Taken as a whole, these sessions, which precede hands-on testing of the plan, should provide an unbiased evaluation of how well the business continuity plan would protect essential locations, business processes, people, and technology. After conducting the exercises, management should identify ways to improve the plan.

Step 3: Develop a business continuity management infrastructure. 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 crisis or disaster. Essentially, it's the internal organization that administers 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 activities during an incident. What is equally important, but often overlooked, is that there should be guidelines for quick, accurate, and appropriate notification of third parties, such as media, shareholders, police, regulators, and public utilities. Just by creating this infrastructure, 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 frequently their companies actually suffer potentially serious disruptions, a measure that is difficult to obtain without an infrastructure. (After implementing an incident management infrastructure, one insurance giant recently found that in a six-month period it faced 29 major interruptions and more than 300 minor outages.)

> "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."

Step 4: Train employees in crisis management. There should be a formal, written plan that educates employees responsible for continuity planning and crisis or incident management. A series of mandatory classes with a curriculum that mirrors the company's business continuity plan is the best way to ensure that employees are taught practical knowledge that will fit with the internal procedures to deal with disruption. 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 management best practices by being active in such groups as the Contingency Planning Exchange (www.cpe-

world.org). This organization offers educational materials, provides member forums, and helps set broad standards for business continuity issues.

Step 5: Establish metrics. High benchmarks for corporate business disruption preparedness and recovery must be set to ensure that the continuity plan and the incident 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.

> "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."

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. +

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

"Security and Strategy in the Age of Discontinuity: A Management Framework for the Post-9/11 World," by Ralph W. Shrader and Mike McConnell, *s+b*, 1Q 2002. www.strategy-business.com/article/?art=228408

"From New Economy to Siege Economy: Globalization, Foreign Policy, and the CEO Agenda," by Jeffrey E. Garten, *s+b*, 1Q 2002. www.strategy-business.com/article/?art=229483

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

Booz | Allen | Hamilton