Tactical Guidelines, TG-14-5298
Research Note
20 September 2001

D. Scott, B. Gassman

The Ripple Effect: Disaster's Indirect Impact

The events of 11 September 2001 show that disasters affect even enterprises far from the scene of the event. Enterprises must begin preparing for these ripple effects immediately.

Core Topic
Security and Privacy: Security Management Strategies and Processes

Key Issue
What strategies should enterprises employ to provide business process protection in the event of a disaster?

Tactical Guidelines
Enterprises should immediately evaluate the effectiveness of their business continuity programs in responding to secondary effects of a disaster. This evaluation should include ensuring that the scope of the program includes all plan components:

- Disaster recovery
- Business recovery
- Business resumption
- Contingency planning
- Crisis management

The horrific terrorist attacks on the World Trade Center and other targets on 11 September 2001 affected enterprises far from the immediate location of the attacks. The national, and indeed global, consequences of these attacks show that enterprises must undertake comprehensive business continuity planning to prepare for the indirect impact of disasters.

Internet Overload

Many enterprises found their Internet access points overloaded with traffic after the attacks, because personnel were using the Internet to get up-to-the-minute streaming news coverage of the disaster and to send e-mails to family and friends. In fact, Internet-based messaging, such as e-mail and instant messaging, was frequently the only effective means of communication immediately following the attacks, because telephone circuits in the affected areas were often overloaded or otherwise unavailable.

Users' Internet services, such as Web and e-mail access, are important tools for enterprises attempting to manage and recover from a crisis. However, e-mail and other Internet-based services should also be a key component of the communications plans that will enable enterprises to contact and locate their personnel during and after a disaster. The most effective strategy for the protection of these services is the use of multiple geographically dispersed Internet gateways connected to independent Internet backbones. This approach provides connectivity resiliency during a crisis, and also distributes load during normal operations.

The events of 11 September point to another problem with Internet access during a disaster: the greatly increased volume of nonbusiness-related activity often clogs networks, preventing or limiting their use for legitimate business operations. Few enterprises would want to block streaming news coverage in the event of a disaster, but they must nonetheless ensure adequate bandwidth for the continuation of critical business operations. One way to achieve this goal is through the use of policy-based networking equipment — e.g., proxies, uniform resource locator (URL) filters, firewalls and bandwidth shapers — which can keep specific users or applications from overwhelming Internet connections.

An appropriately configured network policy can enable enterprises to allocate enough bandwidth to ensure that critical business functions requiring Internet connectivity are protected during a crisis. Many enterprises will, however, find it difficult to determine the Internet access — i.e., bandwidth — requirements of specific business processes and applications. Understanding the resource dependencies of critical business processes is a vital part of business continuity planning. Gartner therefore recommends that enterprises consider the use of Internet access gateways when updating their business impact assessments, and plan for appropriate recovery strategies.

Loss of Transportation Systems

In the aftermath of the 11 September attacks, most enterprises were affected by the loss of transportation systems. They found themselves scrambling to aid stranded employees who needed to return home from business trips, unable to ship products by air, and unable to ship documents by overnight mail. One particularly significant impact was on payroll processing: Many enterprises found that their usual overnight shipments of paychecks (for those employees not paid by direct deposit) could not be made, and, consequently, many had to rush to set up one-time electronic payments. Other enterprises invoked their established disaster recovery plans and printed paychecks in decentralized locations where their employees could pick them up.

Impact on Business Partners, Suppliers and Service Providers

After the attacks, many enterprises found that their business partners, suppliers or service providers — many of which were located in or near the World Trade Center — had been adversely affected. Those that had effective business continuity plans in place will recover and return to delivering services; however, the time and extent of the recovery are often specified by contract. Ensuring business continuity is expensive, and enterprises that do not specify requirements in their third-party contracts are not guaranteed continued services, let alone specific levels of service. Best practices require that business continuity requirements be spelled out in contracts with third parties, along with testing frequency — including enterprise participation.

The Need for Better Contingency Planning

Contingency planning is the component of business continuity planning that focuses on preparing for external events that could interrupt a critical business process and thereby damage the enterprise. Such external events include: loss of a critical supplier, failure in the financial flow (e.g., funds transfer), loss of senior executives or other key personnel, and loss of transportation systems. Of the tens of thousands of enterprises directly or indirectly affected by the 11 September terrorist attacks, few were fully prepared to deal with such contingencies. Gartner estimates that just 10 percent to 15 percent of large enterprises — financial services providers excepted — have up-to-date contingency plans, and the percentage is even lower for smaller enterprises. A crisis is not the time for planning; it is the time for execution of the already-defined plan. The absence of adequate plans hampers recovery efforts, with the result that enterprises require significantly greater time to recover — if they are able to recover at all.

Bottom Line: A disaster inevitably results in ripple effects on other enterprises — even those that may be at a considerable distance from the location of the disaster. Gartner recommends that enterprises respond to the threat of such secondary effects of disaster by immediately evaluating the effectiveness of their business continuity programs. This evaluation should include ensuring that the scope of the program includes all plan components: disaster recovery, business recovery, business resumption, contingency planning and crisis management.