NATIONAL INFRASTRUCTURE PROTECTION CENTER

HIGHLIGHTS

A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.

Issue 11-01
December 7, 2001

Editors: Linda Garrison
Martin Grand

! **September 11, 2001, Terrorist Incidents Lessons Learned: New Approaches Needed for Disaster Recovery and Business Continuity Planning**
! **Terrorists and the Internet: Publicly Available Data should be Carefully Reviewed**
! **Domain Name System: Eliminating Single Points of Failure**

For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or (202)323-3204.

We welcome your comments and suggestions for improving this product. To provide comments, contact the Editors at (202) 324-0334 or (202) 324-0353.

This issue has an overall classification of Unclassified. This publication may be disseminated further without express permission.

September 11, 2001, Terrorist Incidents Lessons Learned: New Approaches Needed for Disaster Recovery and Business Continuity Planning

Three major themes can be noted in the many articles in which technical professionals have been discussing the impacts of the September 11 incidents.

Emerging Lessons

First, the disaster recovery plans of most organizations tend to focus on information system availability ("up-time") issues. Second, the evolving understanding of the scope of the impacts has resulted in a fundamental reassessment by both private sector and government organizations of the meaning of "worst case scenario". Third, and most important, there appears to be an emerging synthesis of the two first themes: the incidents have resulted in an increasing awareness of the need for business continuity plans and disaster recovery plans to complement each other.

Financial Services Infrastructure

Many large financial service organizations quickly restored their information systems at alternate sites. The systems demonstrated stability under high transaction volumes as markets reopened and business resumed. Factors contributing to successful resumption of operations include investments in real-time data backup and full hot site capabilities, frequent disaster plan testing and updates, lessons learned during Y2K remediation and other plans for critical functions such as NASDAQ's decimalization conversion plan.

Traditional disaster recovery services pushed to new limits

Companies offering disaster recovery services have reported record numbers of organizations submitting disaster alerts and disaster declarations. Furthermore, in many cases the nature of the services required is also significantly broader than in previous disasters such as Hurricane Floyd in 1999 and the 1993 World Trade Center attack.

Need to reevaluate risk issues

During the last 15-20 years, focus on cost-cutting and productivity increases has contributed to consolidation of organizational operations, information, people, processes, and supply chain relationships. The September 11 incidents show these trends present new potentials for failures that have not been reflected in many disaster recovery and business continuity plans. Additionally, the incidents also point out risk factors related to close proximity to other "high value targets" and cross-infrastructure dependencies on telecommunications, power, and transportation.

Critical Infrastructure and Enterprise Network implications

The basic principles of emergency readiness have been used for decades and can continue to be a basis for addressing new challenges. However, two new planning approaches need to be addressed. First, the scope of disaster recovery planning must be broadened beyond its traditional focus on primarily operational issues to include backup security measures as well. Second, business continuity planning combined with disaster recovery planning needs to be approached as an enterprise-wide business operation requirement.

Terrorists and the Internet: Publicly Available Data should be Carefully Reviewed

Risk management should be considered when reviewing materials for web dissemination, balancing the sharing of information against potential security risks.

Our nation's heightened threat environment has highlighted concerns that information posted on the Internet regarding critical infrastructures could be used to aid in malicious activities. In light of this awareness, there have been numerous efforts to remove such sensitive information from relevant web sites.

These actions, however, have touched off a debate concerning freedom of information. For example, some of the data that was removed by the Environmental Protection Agency (EPA) concerned the locations of 15,000 chemical sites around the nation. Many argue that citizens have a right to know this type of information and it should remain publicly accessible.

When reviewing data, security concerns may not always be obvious. For example, a particular piece of information may seem harmless, but when used in conjunction with other publicly available data, the aggregate could be useful for those with malicious intent.

Factors to Consider

When posting info to the web or reviewing current content, it is important to consider the following:

- Has the information been cleared and authorized for public release?
- Does the information provide details concerning enterprise security?
- Is any personal data posted (such as biographical data, addresses, etc.)?
- How could someone intent on causing harm misuse this information?
- Could this information be dangerous if it were used in conjunction with other publicly available data?
- Could someone use the information to target your personnel or resources?

Finally, risk managers should realize that many archival sites exist on the Internet, and that information removed from an official site might nevertheless remain publicly available elsewhere, such as that appearing on mirrored sites by private entities.

Domain Name System: Eliminating Single Points of Failure

Companies need to examine their domain name service architecture to avoid creating a single point of failure that can result in an extended loss of connectivity.

The Domain Name System (DNS) is a distributed catalog that allows users to access Internet resources by using familiar text strings like WWW.NIPC.GOV instead of difficult numeric addresses like 32.96.111.131. An organization establishing an online presence will generally specify two or more name servers that provide authoritative DNS information. If DNS becomes unavailable, access to common resources such as web browsing, e-mail, remote login capability, and other fundamental Internet services can be totally disrupted. In this sense, DNS can be a single point of failure presenting a risk of total loss of electronic connectivity for a company.

In early 2001, a major U.S. technology firm experienced widespread connectivity problems when a technician mistakenly re-configured a router to block access to the firm's DNS servers, all of which were located on the same network segment. The outage was subsequently exacerbated by a malicious denial-of-service (DoS) attack mounted against that part of its network, further blocking access to the company's DNS servers.

Factors Increasing Risks Associated with DNS Failure

- **Lack of Redundancy.** Some organizations provide the same address for both primary and secondary name servers, making them completely dependent on the reliable functioning of a single server.
- **Incorrect Configurations.** Some organizations have failed to list all of their DNS servers in their domain registration records, or they have made configuration errors which result in only one name server having authoritative DNS information.
- **Architectural Flaws.** If all of an organization's name servers are located on the same physical network segment, a fiber cut, a routing misconfiguration, or a DoS attack can make all of them simultaneously unavailable, totally disrupting DNS.

The Icelandic network consulting firm Men & Mice, which conducts periodic surveys of DNS health, has reported that a surprising number of online firms exhibit one or more potentially serious DNS problems. For example, 25% of the large corporations it recently surveyed appeared to host all of their name servers on the same network subnet.

Any critical infrastructure provider which is dependent upon Internet access needs to review its DNS architecture to ensure reliable functioning of this service. Particular attention should be paid to adequate redundancy and physical dispersion of the organization's name servers so as to avoid a single point of failure. Both of these issues can be resolved in a variety of ways, including dispersing name servers across geographic locations, arranging for mutual backup DNS service with another company, or contracting with a third party to provide additional name servers.