

After the Attacks: Plan for New Internet Security Measures

John Pescatore

The recent terrorist strikes — and the anticipated reprisals — dramatically increase the risk of cyber attacks. Enterprises should prepare for more assaults and increased Internet security requirements.

NEWS ANALYSIS

Event

On 11 September 2001, a series of terrorist attacks using hijacked commercial aircraft destroyed the World Trade Center in New York City and severely damaged the Pentagon in Arlington, Virginia, a suburb of Washington, D.C.

Analysis

The recent terrorist attacks on U.S. targets have taken a devastating toll on human life and physical property. However, this disaster will also have near term-impacts on cyber incident levels, and some longer-term effects on Internet security practices.

Any military reprisals the United States makes will inevitably lead to cyber attacks against U.S. government, financial and political Internet sites, as well as similar sites in countries seen as supporting the United States. Most attacks will come from hackers and activists using these events to disguise simple vandalism and site defacement. However, more targeted attacks — including full-scale denials of service — should also be anticipated.

Enterprises should take the following actions:

- *Immediately* check their Internet-exposed systems and servers for vulnerabilities and test their cyber incident response plans — Not only must their IT assets be kept safe from direct cyber attacks, but steps must also be taken to keep enterprises' own servers, and remote PCs, from being used as launching points for attacks.
- If revenue-producing or other business-critical operations depend on Internet connectivity, enterprises should begin budgeting for contractual denial-of-service protection from their Internet service providers (ISPs) or Internet data centers.
- If enterprises use computing facilities outside North America as their primary Internet connections or computing centers, they should begin preparing for backup operations at North American sites — particularly if these computing facilities are located in the Middle East or elsewhere in Asia.

Enterprises should also expect the following:

- Longer-term Internet-security effects will result, including greater law-enforcement and intelligence-community demands for Internet surveillance in every country of operation.
- Attempts to place stringent export controls on strong encryption technologies — so far largely ineffectual — will probably be revived.
- The U.S. government will likely propose the imposition of encryption key escrow schemes that support real-time surveillance, at least at ISPs. However, we do not anticipate any near-term effect on enterprise use of encryption technologies such as virtual private networks (VPNs) and Secure Sockets Layer before the second half of 2002 (0.8 probability). Telecommunications and managed VPN service providers should prepare legal, policy and technical responses to such demands.

Analytical Source: John Pescatore, Information Security Strategies

Written by Terry Allan Hicks, gartner.com

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509