

White Paper: The Internet

“Disaster Recovery Issues & Answers”

Tari Schreider

The Disaster Recovery Practitioner’s Resource

As originally conceived, the Internet was a technological revolution in information gathering and dissemination. High-speed data links and packet switching allowed mail and file transfers between a small group of government and university computer systems. Today, the Internet is a global network connecting tens of thousands of computers and more than 30 million users throughout the world. Any Disaster Recovery Practitioner (“DRP”) with access to a PC and a modem can now roam the Internet and gain access to literally thousands of sources of essential disaster recovery and risk management information.

With the World Wide Web (“WWW”) at their fingertips, DRPs can call-up the Home Pages of organizations which provide valuable information ranging from earthquake preparedness to locating disaster relief agencies. DRPs can download vital information from these Home Pages to create and/or enhance their own contingency planning efforts. Using an Internet Browser, a DRP can access on-line Search Engines to drill-down to topics as specific as hot sites or sources of disaster recovery education. The Internet is truly an indispensable tool for any DRP.

Worthwhile WWW Home Pages

The Internet contains nearly 12,000 sites

which hold information on emergency management, risk management, disaster recovery, and security. DRPs can have access to the same information that the major disaster recovery consulting firms do if they invest their time in a little “Data Mining.”

DRPs should maintain their own favorite places on the WWW and organize them in the following categories:

- Plan Development Sites, e.g., Disaster Recovery Journal, Insurance Industry Association, etc.

- Risk Management Sites, e.g., Hazard Reduction & Recovery Center, etc.

- Disaster Response Sites, e.g., American Red Cross, FEMA, etc.

- Security Management Sites, e.g., CERT, MegaMall - Safety & Security

Document the addresses of all your WWW sites along with all your other emergency contact information.

Backing Up/Restoring Critical Data

Backing up PC and network data is certainly nothing new. However, using the Internet as an enabler to backup and restore critical data is relatively new. A number of companies have already emerged offering services for backing up and restoring data over the Internet. Subscribers to these services would download the backup/restore program from a service providers WWW

site, and then register on-line. Once registered, users would specify a daily backup schedule, after which the service would begin performing the on-line backups automatically. The backup can also occur over a private dial-up network if access to the Internet is not available. Multiple passwords as well as DES encryption to ensure data security are an integral part of these services. The client’s data is stored at case-hardened mirrored operations centers, each with multiple levels of data redundancy.

In the event of a disaster, users could retrieve their backed up data over the Internet and restore it at a hot site or other recovery location. Costs for these types of services are usually based on the quantity of compressed bytes of data backed up, type of archival media (CD-ROM, DAT, etc.) and a monthly service fee.

Table 2 lists some companies which offer products/services for backing up and restoring data over the Internet:

Commercial Internet Recovery Services Emerge

Recognizing both a financial opportunity and market need for a recovery solution designed around the Internet, hot site providers are now rolling-out Internet recovery services. IBM was one of the first to announce an Internet recovery service through their partnership with Icon CMT Corp., one of the

largest Internet Service Providers in the United States. IBM's service is designed to recover WWW applications in the event of a disaster. Through their offering, IBM can reestablish the connection to the client's critical Internet-based applications, allowing the client's user community to continue to access the applications following a disruption. IBM will reestablish the Internet link by redirecting the Internet traffic to its Sterling Forest, NY recovery facility using the IBM Global Network and Advantis. IBM provides the network equipment that enables the client to connect their systems to the IBM network.

Another service emerging from systems integrators, hot site providers, and VAR's is an Internet Emergency Response Service. These offerings include security testing of the Internet links, virus sweeps, employee awareness training programs, security policy implementation, and incident response during a breach in security or a disaster event.

Internet Security Concerns Abound

One of the most publicized aspects of the Internet has been the universal concern over

the lack of security. There are two primary security concerns associated with the Internet. The first involves concerns over the threat of hackers accessing your company's system through the Internet connection. The second involves the sanctity of the data once it is sent across the Internet and who can actually view and/or intercept it.

These concerns are certainly not unfounded as stories of hackers breaching Internet security continually hit the front pages. One of the more famous incidents was Kevin Mitnick's hack into the Internet Service Provider Netcom Communications Corp. in San Jose, CA where he stole over 2,000 credit card numbers.

The most effective way to protect your company from outside intruders is to implement a fire wall at your company site. Fire walls range in sophistication from simple protocol filters which restrict data traffic to and from the Internet, to advanced fire walls which control the types of packets that can actually move in and out of your system. If the concern leans more toward the security of the data being transmitted, data can be encrypted at multiple levels. Security measures include securing traffic between network nodes using Internet Protocol ("IP") level encryption software or encrypting data at the session level by securing the Sockets to ensure that text and graphics can be encrypted prior to being sent to a browser.

As your company's DRP, you must work closely with your security administrator to assess the vulnerability of your company's network and then implement a risk reduction strategy and program to identify and then mitigate breaches in security. Remember, in a networked world, the most likely risks you'll have to combat will be breaches in security, not natural disasters.

Viruses On The Internet

Computer viruses are becoming a growing concern on the Internet. Gone are the days when virus writers were simply amused by developing infectious programs which would spread inside computer programs or the boot sector of a floppy disk. Today, there are new, insidious form of viruses which at-

Home Page	Address	Site Description
ACM: The Risks Digest	http://www.catless.ncl.ac.uk/Risks/index.1html (substitute "1" with 2 - 100 to access other volumes)	Digest of articles produced by ACM Committee on Computer & Public Policy. Indices provide access to disaster, risk, and security related articles, papers, and press releases.
The Chubb Corporation: Insurance Library	http://www.chubb.com/library.html	Source of information about all types of insurance policies, claims procedures & other related topics.
Disaster Recovery Journal	http://www.drj.com	A source of DR research, articles, seminars, and hot-links to recovery service providers. Chat Forum provides an opportunity to communicate with other DRP's.
Emergency - A guide to the Emergency Services of the World	http://www.catt.citri.edu.au/emergency/emergency.html	WWW guide to sources of emergency services throughout the world. Provides hot-links to hundreds of other disaster recovery sites.
The Emergency Response & Research Institute	http://www.emergency.com	Central source for EMS, Fire, and Police emergency services. Covers disaster/rescue, hazardous materials, terrorism, natural disasters, and many other areas.
Federal Emergency Management Agency (FEMA)	http://www.fema.gov	Provides fact sheets on all types of disasters which provide details on hazard mitigation and response. The Federal Response Plan details the government's reaction to national and regional disasters.
Hazard Reduction & Recovery Center	http://www.archone.tamu.edu/centers/hrrc.html	Largest research center in the world chartered to study the effects of natural and technological hazards. Specific topics include emergency planning and response, crowd behavior, and sheltering systems.
NACEC Disaster Support Services	http://www.nacec.org/disaster.html	Provides rapid response logistical communications support for large scale disaster relief operations within North America.

Table 1

tach themselves to programs or files downloaded using FTP's that are invading clients and web sites alike. As you're reading this, virus writers are now developing new strains which can attach and infect Internet Java and OLE

created applets which could theoretically be carried to millions of client sites throughout the world. The new open distributed computing environment will allow platform independent viruses to proliferate throughout the WWW.

Internet virus software is designed to run as a dedicated scanning station which is positioned behind the fire wall. This new generation of virus software checks FTP (File Transfer Protocol) downloads and SMTP (Simple Mail Transfer Protocol) e-mail. The emergence of these new anti-virus packages is a direct assault on the unconstrained macro viruses which are wreaking havoc on networks throughout the world.

Companies which offer Internet-based virus software are featured in Table 3.

Could Your Internet Service Provider Disappear?

Imagine receiving a phone call one Saturday morning and being awakened with the news that your company's Internet access no longer existed. That's exactly what happened recently in Salt Lake City, UT as the sudden demise of InteleNET, a local Internet Service Provider ("ISP"), left 1,200 companies without the ability to read their e-mails or their customers the ability to access their web site's Home Pages. Another case just a few months earlier occurred in Atlanta, GA when RandomAccess, another local ISP was robbed at gun point while stunned employees watched as the thieves pillaged every web server in search of their memory chips.

RandomAccess estimated the loss at nearly \$1 million. In this case over 500 com-

Product:	Provider:	Contact:
DataSafe	Connected Corporation	(888) 9-BACKUP
Rimage Televaulting	Rimage Corporation	(800) 445-8288
SafetyPosit	Software Partners/32	(508) 887-6409
WebStore	MacAfee Associates	(408) 988-3832

Table 2

panies lost Internet access for nearly a week.

Although few companies have placed their strategic applications on the Internet, many do nonetheless rely on the Internet. If your company is among those that do, you need to have a recovery strategy in place in the event that your company's ISP disappears. First begin by checking the financial background of the ISP your company currently uses and make it a biannual procedure if your ISP is a startup. Next, have your ISP provide you with a copy of their disaster recovery plan to verify if they could (at the very least) survive the most likely outage scenarios. Focus in on how your Home Page and account information is backed up. Request that you also receive backups of any critical web site data. It would also be prudent to have a relationship with a secondary ISP that you could quickly switch to in the event your primary ISP experiences a disaster. Ensure Home Page compatibility and have a procedure in place to notify your clients through an e-mail broadcast or other form of communication of the new number and address at which they can contact you.

Product:	Provider:	Contact:
InterScan	Trend Micro Devices	(408) 257-1500
Norton Antivirus	Symantec	(408) 253-5000
SecureWay	IBM	(800) 742-2493
WebShield	MacAfee Associates	(408) 988-3832

Table 3

Will The Internet Crash & Burn?

For all the promise the Internet holds for changing the way business does business, there is a looming dark side. With 30 million users and 110,000 web sites increasing exponentially, the Internet is consuming bandwidth faster than it can be increased. The

success of the Internet rises and falls on the comparatively narrow bandwidth of the public switched network which connects clients (users) to the servers (web sites).

Already parts of the country have been and will continue to experience "capacity-brownouts" where users who once found e-mail messages sent in a matter of minutes now take a matter of hours. Bandwidth, however, is not the only limitation facing users of the Internet. There is already a shortage of class 2 and 3 IP addresses.

According to the technology research firm International Data Corp., there will be 200 million users on the Internet by the year 2000. With no one organization in charge and an estimated price tag of several billion dollars to create the Information Superhighway with virtually unlimited bandwidth, the future of the Internet is unclear. Ironically, the physical structure of the Internet is quite robust. After all, the Internet was originally designed by the Department of Defense to take a licking and keep on ticking in the aftermath of a nuclear attack.

With the Internet a "Hackers Paradise", Service Providers failing, and bandwidth shortages increasing, the Internet is wrought with perils. DRP's need to be intimate with Internet technology and software in order to effectively design risk management and

recovery strategies. The recovery needs of the Internet are distinctly different from that of the "Glass House." Don't let your company end-up as road kill on the In-

formation Highway just because you don't have an Internet recovery plan!

Tari Schreider is the Director of Research for Contingency Planning Research, Inc.

This article adapted from Vol. 9#3.