COMPUTERWORLD

What will you do when the cyber-levee breaks?

Bruce Levinson

September 21, 2005 (CIO)

Hurricane Katrina will lead to endless finger-pointing about what should have been done to strengthen the levees before the storm.

However, as a former senior FEMA official under the Clinton administration explained, "There's only two kinds of levees: Ones that have failed and those that will fail." The same is true for cyber-levees.

The Internet today is in the same position as New Orleans was before the hurricane, a heavily fortified resource of incalculable economic and cultural value whose protections will one day inevitably fail.

The above observation does not mean that there should be any slackening of efforts by all stakeholders to continue strengthening cybersecurity protections. Governments, industry, academia, and individual computer users will always need to take vigorous measures to protect both the Internet and their own data.

However, everyone should realize that there are limits and fallibilities to even the mightiest efforts.

Not only are there limits to how far we can go in securing the Internet, there should be limits. After all, the most secure computer is one that is unplugged. Enjoying the social and economic benefits of the Internet also inherently means accepting and learning to manage risk.

Just as the world was shocked by the devastation of New Orleans, a scenario that has been predicted for decades, so too will the globe be staggered by the failure of the Internet. There are still many people and institutions who don't appreciate just how intertwined the Internet has become in virtually every aspect of modern society.

New Orleans will eventually be rebuilt in some form. The Internet will most likely be repaired much more quickly. However, the consequences of each failure will reverberate long after working infrastructures have been restored.

What is needed is not just to protect the Internet but also to prepare for the time when those protections fail. In addition to the usual contingency planning processes, two extra steps would be helpful in getting ready for a really bad day.

Making sure your data is regularly and securely backed up in geographically diverse locations, having hot sites, cold sites and all the other associated tools, services and miscellaneous paraphernalia are important aspects of disaster preparedness. But it's not enough.

One of the lessons learned from Katrina and 9/11 is that communications failures are the first

consequence of disaster. Radios fail. Cell phone networks become overwhelmed. Plain old telephone service goes down. Since the Internet is really nothing more than a means of communicating, Internet-disaster planners should recognize that what you are going to experience is a failure to communicate.

Depending on what causes a major disruption (natural disaster, violence, cyber-attack) it would not be surprising to see virtually all non-human communications networks fail, including phones, cell phones and even local wireless networks. One way to prepare for communications failure would be to have backup or workaround systems available that could range from satellite phones to manual typewriters.

However, an additional option for disaster preparedness is to revive the term *plenipotentiary.* Derived from the Latin words *plenus* and *potens, plenipotentiary* refers to a person who has full and independent powers to act on behalf of an organization. Most commonly applied to select ambassadors prior to the era of rapid global communications, plenipotentiary officials were authorized to act on behalf of their government without having to check back with the home office.

Thus, the first component of an Internet-failure strategy includes selecting an official at each location who would be in complete charge of the situation and fully authorized to take whatever actions he deems necessary--including those that are not in any plan.

The obvious choice for designated plenipotentiary official would be the senior administrator at each local or regional office. However, the most senior person is not necessarily the best crisis leader. An organization may or may not need to take the uncomfortable step of selecting someone other than the local head honcho to take charge during an emergency. Pick someone who is good at improvisation and knows how to lead.

Conventional wisdom says that once you have someone with the power to act, it might help if he knew what to do. Conventional wisdom is all well and good but often incomplete. You don't need a man with a plan; you need someone who knows what to accomplish as well as what to do.

Contingency plans are great at providing lists of steps for people to take during various scenarios. They rarely explain what to do when the situation doesn't fit of one the prepared scenarios or if you can't take one or more of the listed steps. Plans don't always fail but that is a reasonable way to bet.

Part of developing an Internet-failure strategy involves one or more senior officials figuring out what needs to be accomplished in the event of network failure, what can be accomplished under such circumstances and then developing some basic goals and guidance for the local crisis managers. Devising such guidance has the potential to be a major organizational undertaking. Conversely, it may be possible to draft effective guidance on the back of the proverbial envelope. Regardless of what developmental approach is used, try to do it without PowerPointing everyone to tears.

A broader initiative is needed for the second step in preparing for the day you would prefer occurs on someone else's watch. It's good to be able to bounce ideas off other people, particularly off people who have different backgrounds, perspectives and responsibilities.

A forum should be instituted that includes representatives from industry, academia, think tanks and all levels of government. The goals of the forum should be rather modest. Attempts to set standards or develop common Internet-failure plans would only result in the promotion of narrow institutional interests.

Instead of seeking "solutions," the forum should focus on ventilating ideas. Irrespective of whether any consensus emerges, the very process of discussing concerns, views and suggestions would prove valuable to the participants.

Given time and budget constraints, it's not practical to create yet another formal organization.

What will you do when the cyber-levee breaks?

There are already enough professional associations, trade associations, standard-setting organizations, planning groups and the like. Instead, use the Internet to get ready for the lack of an Internet.

Most football, cooking or car fanatics are likely members of at least one Internet forum. It should not prove too difficult for a company or think tank to establish a freewheeling Internet forum on Internet failure. CIOs and others could participate as time permits and ideas occur. No need to hire staff, prepare agendas or buy more plane tickets. The only reason to meet in person would be to party like there's no tomorrow.

So get ready for when your cyber-levees fail, since, as the former Robert Zimmerman explained, a hard rain's a-gonna fall.

Bruce Levinson is director of the CyberSecurity Policy Project at CyberSecure.US, an affiliate of The Center for Regulatory Effectiveness.