Contingency Planning Must be Comprehensive

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In a recent column, I pointed to the free, Web-based _CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS _ edited by Elizabeth B. Lennon and published by The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) (available at <http://csrc.nist.gov/publications/nistpubs/index.html>).

One of my regular correspondents contributed this analysis of the document based on his extensive professional experience.

* * *

The NIST plan simply reinforces the mistakes that have been made in government contingency planning over the years. No one but IT had a plan – if there was any plan at all. Even if one existed for IT, it usually would not work since it was not properly tested.

As late as the late 1980s, the Office of Management and Budget (OMB) was turning down funding requests for contingency plans for mission critical government systems like Veterans Administration (VA) benefits because the risk assessment wasn't adequate. So VA gave them a risk assessment (really more of a business impact analysis) explaining why vets need their benefit checks. To this day, there is still no adequate contingency plan for veterans’ benefits. Their master records are stored and processed on a Honeywell system using GCOS VIII. Try to find another one of those somewhere.

While working as consultants in the late 1990s, some of my associates tried to get another agency to test its contingency plan. They were too busy with other things. If the plan did not work, it meant that important income maintenance might well not be available to people in need.

At another important agency that deals with economic analysis, a consultant entered the equipment inventory for the data center into a specialized database and also did a business impact analysis. They thought they had a contingency plan; however, they did not do the telecommunications part. They certainly needed a good plan, since the people who designed their data center decided to put a glass wall on the front with windows so you could see into the computer room. This was designed after the WTC and OK City bombings.

We have learned very clearly since 9/11 that technology-based plans, even if tested, are useless without the people to use them. That means not just the technology people but the business people too. People need a place to work after an event destroys their original office space.

Although the NIST document makes mention of other types of plans such as crisis management and business recovery, it does not attempt to offer even brief examples or provide links where the reader could get more information. The NIST document simply encourages the types of inadequate, localized, technology-oriented contingency plans which have been developed both in
government and industry. These proved less than adequate for organizations facing the recovery processes after 9/11.

GAO has issued a review of Federal Deposit Insurance Corporation (FDIC) Computer Security subtitled “Improvements Made but Weaknesses Remain” and dated July 2002 (GAO-02-689; see <http://www.gao.gov/new.items/d02689.pdf>). Some of the additional improvements it recommended for the FDIC contingency plans include the following:

1. Use unannounced tests or walk-throughs because real disasters give little if any warning;
2. Develop business continuity plans for _all_ facilities;
3. Deal with the potential unavailability of a backup computer facility, as happened to some such facilities in the Washington DC area on 9/11.

It seems easier to convince IT managers of potential threats, since they see the hits on their firewalls daily and most are keenly aware of the need to keep anti-virus software updated; getting business managers to face up to the potential for physical attacks is much more difficult.

Some places have excellent system and network security. They may even do a fair job at personnel security. But they neglect physical security, providing that weak point in the perimeter for potential attackers. Since these different areas of security are usually in separate organizations, it's difficult for anyone except at very high levels to see the big picture. Unfortunately, most of the senior officials are not interested in these types of risk, assuming that the responsible managers have everything under control. Often that is not the case.

My rule is that your physical security should be able to stop, at the building perimeter, an irate ex-husband or a disgruntled ex-employee, even if they are armed. If you can do that, you will at least slow down even a well-trained terrorist team.

We all need to plan for the worst case that we judge likely. That means comprehensive plans that address technology, people and facilities and constant monitoring to keep the plans up to date as conditions change. Anything less, and it won't work.

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without
limit on any Web site, and to republish it in any way they see fit.