I have been inviting friends and colleagues to send me interesting essays for this column. Michael Miora, whom I have known since we worked with the old National Computer Security Association starting in the early 1990s, has very kindly sent me the following text. As usual, I’ve done some light editing and added some references for further reading.

* * *

How has the landscape of incident management changed since September 11, 2001, and how will we approach the subject in 2003?

There are few statistically and methodologically sound surveys addressing the question of how companies face and handle incident management and how this has changed in the last year. However, the “Preponderance of Anecdotes” will help us find the answer.

There is good news. In the last year, we have seen that those companies who had already addressed the issue before 9/11 have often improved their incident management posture. Plans that were previously in place and tested have often been reviewed in detail, expanded, updated and retested. Some systems and functions that were previously excluded because they did not seem worthy of protection have been brought under the incident-management umbrella. Moreover, organizations have begun to realize that they must take extraordinary precautions to protect their employees; as a result, emergency preparedness measures such as food, shelter, transportation, family communication, and other such measures have been greatly improved in many companies we have seen.

There is also bad news. Generally, organizations that were unprepared and unprotected before September 11, 2001, are for the most part still unprepared and unprotected. Our tough economic times compound the difficulty of making planning a high priority even though terrorism, cyber attacks, and other incidents make news daily. The biggest problem planners tell us that they face is justifying the cost, which they must do in a quantifiable, Return-on-Investment (ROI) basis.

The most important news is the growing receptivity of executives and middle management to the idea that incident management should be a key part of the corporate infrastructure. We have seen and heard top management report that this is now a concern that is raised regularly in the boardroom and at management working meetings just as it has been an important topic in the computer and telephone rooms. That growing interest and openness represents a major new opportunity for the incident-management planner to get funding for viable and cost-effective disaster recovery and incident response plans.

The opportunity is to define well-segmented plans that protect key elements against high-probability events at low cost. Our newly receptive audience is cost conscious and recognizes
that both short-term profit and long-term profitability are dependent upon containing costs. We must show them that these segments, once built and tested, can then be leveraged to lower the cost of future extensions of the plan.

It is critical to show clearly that during the coming 3-5 year period, depending on the company and industry, the cost of preparation is lower than the cost of incident handling without a plan. This explanation cannot be a probability-based argument where the large cost of a major natural disaster is modified by a probability of occurrence. Instead, we have to show a reasonable basis for predicting that handling any incidents without a plan is bound to be more expensive than the total cost of preparing, rehearsing and refining incident response plans for the same scenarios.

The incidents we plan for don’t have to involve headline news such as hurricanes and tornadoes or cyber- and terrorist attacks. Devise your incident management planning to appropriately include ordinary events and circumstances that happen regularly, causing outages and losses; the cost-benefit tradeoff will come together nicely.

With such an argument in place, it will be possible to show management that implementation of a plan will reduce costs rather than raise them.

Who can argue against saving money?

***

For further reading:

Collection of Recent News and Events in the Incident Management Area
http://www.contingenz.com/infocenter.htm

Companies Snooze on Cyber-Security, BusinessWeek Online, September 10, 2002
http://www.businessweek.com/technology/content/sep2002/tc20020910_7073.htm

Attitudes: The single biggest change, Computerworld, September 9, 2002
http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,74049,00.html

Survey Shows Data Security Work Lagging, Computerworld, September 6, 2002
http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,74074,00.html

Three White Papers on Incident Management
http://www.contingenz.com/whitepapers.htm

***

About the Author

Michael Miora, CISSP, is a renowned incident management and security expert. He wrote chapters on business continuity planning and disaster recovery planning for the _Computer Security Handbook, 4th Edition_ and is an Adjunct Professor in the Norwich University MSIA program. He currently serves as President of ContingenZ Corporation (www.contingenz.com), offering companies incident management consulting and training. He may be reached at <
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@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 Michael Miora & 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.