Disaster Recovery Planning Encourages Better Management Decisions

by M. E. Kabay, Ph.D., Director of Education, ICSA

We usually think of Disaster Recovery Planning as having benefits when disaster strikes. Having invested all that effort really pays off when the building collapses, the CPU melts, or your CIO goes ballistic and erases all your servers.

In this article, I'd like to emphasize that DPMRP--Disaster Prevention, Mitigation and Recovery Planning--is a tremendous boon to any organization whether a disaster ever occurs or not. DPMRP

- encourages rational allocation of corporate resources;
- fosters improved communications among different sectors and levels of an organization;
- supports team- and morale-building efforts;
- contributes to security awareness;
- by definition, reduces the consequences of accidents or malfeasance;
- by definition, is aimed at reducing the likelihood that certain types of disaster will occur at all.

The main point of this essay is that the process of DPMRP is itself conducive to major organizational benefits. The following sections explore why such benefits accrue to those who plan against disaster.

Rational Allocation Of Corporate Resources

Every organization has to make decisions based on a sound understanding of its resources. Resources include people's capabilities and the tools with which they can implement their decisions. Both types of resources have to be catalogued in detail in all Disaster Recovery Planning exercises. No Disaster Recovery Plan can start without lists of people, their titles, their skills, and their backup personnel. Every Disaster Recovery Plan includes details of operational procedures and their priorities. Even more significant, such catalogs are compiled by interviews with the staff members who actually carry out these duties rather than solely from management-eye perspectives and organizational charts. Finally, all Disaster Recovery Planning teams recognize the importance of keeping their picture of the organization absolutely up to date.

It follows that the results of the Disaster Recovery Planning process naturally feeds into a better understanding of the real, as opposed to theoretical, functioning of the entire organization.

Improved Communications

As organizations grow, the difficulty of communicating effectively among all those who need to know certain information grows non-linearly. Frederick P. Brooks, Jr. identified this problem in his classic *The Mythical Man-Month: Essays on Software Engineering* (1975; Addison-Wesley: Reading, MA. ISBN 0-201-00650-2) when he formulated Brooke's Law: "Adding manpower to a late software project makes it later." The reason is the combinatorial explosion of interactions as the number of people rise in a group. As a simplified rule, remember that the number of pairwise interactions possible in a group rises as the square of the size of the group [the accurate formula is
$n(n-1)/2$ which becomes close to n^2 for large n].

The nature of the Disaster Recovery Planning process forces people to communicate with each other at all stages of the analysis, design and implementation. This factor alone can improve communications within the organization. At the very least, the Disaster Recovery Planning Team should include people from all areas of the organization--sometimes fostering meetings among those who otherwise would be very unlikely ever to speak with each other. By focussing on operations, Team members can develop a sound grasp of each other's working environments, needs, priorities, preferences, work habits, and even specialized vocabulary. All of these gains in understanding can foster better communication among participants.

Team and Morale Building

Any organization can suffer from in/out group hostilities. Such hostility becomes evident when one hears statements like "Yeah, those YYY department folks are really nasty / lazy / demanding / intolerant / crazy." Another form of hostility is prejudice, whether based on gender, race, religion, sexual orientation or administrative level. Such inter-group hostilities are disruptive and counterproductive: people can become emotionally upset and distracted; they can lose their work efficiency and make mistakes; they can quit; and they can become abusive or even physically violent.

Such inter-group hostilities *can* be overcome. Research in social psychology shows that one of the most effective methods for reducing friction among groups is to bring members of the hostile groups into situations where they can work together towards common goals. The Disaster Recovery Planning process is a splendid opportunity to provide common goals and to bring people from many sectors and levels of the organization into a positive collaboration.

Security Awareness

Information systems security is a form of disaster prevention and mitigation. The key element for security is people: people who understand the value of the information they generate, organize, store, retrieve, transform and destroy. Most of the damage to information systems comes from people; over half is guessed to result from ignorance and carelessness of authorized users. Another large part of the threat to information results from the actions of dishonest and disgruntled employees.

Given these realities, employee awareness of security becomes the greatest bulwark against misuse and/or damage to information. Unfortunately, many people view security as a problem rather than as a solution; they see only the increased work load that results from careful consideration of threats and risks. The initial phases of the Disaster Recovery Planning process

provide an opportunity to change people's opinion of security because they have to grapple with the value of information in many different areas of work within the organization. Not only must employees look at the possible consequences of destruction or unavailability of information, but they must also think about the consequences of unintended disclosure of confidential information. It becomes hard to dismiss security after you've spent months thinking about security!

On another level, social psychology teaches us that we tend to internalize the values of any project upon which we work. For example, employees who have participated in Disaster Recovery Planning can come to feel a sense of ownership of the process; they feel in control, they are committed and they act as ambassadors or champions for the project--including security--in the rest of the organization.

Making Accidents And Malfeasance Less Costly

Organizations regularly spend a great deal of money on insurance policies. For example, a high-tech company with about 50 employees can easily spend $8,000 a year simply on damage and liability insurance. Service contracts for $1,000,000 of computer equipment and software currently cost around $100,000 a year (depending on service levels). The same company directors who would never think of going without insurance and support contracts may nonetheless balk at investing in Disaster Recovery Planning. The irony is that the regular insurance policies won't help in any way unless there really is a problem. Investment in Disaster Recovery Planning, like investment in a good preventive-maintenance program, can actually *reduce the severity* of the damage if a disaster does occur.

Considering physical disasters, it's clear that emergency preparedness can reduce the seriousness of accident or attack to negligible proportions. For example, having a good system of smoke detectors can lead to such quick response that no disaster will occur at all. That's the ultimate cost reduction.

Making Disasters Less Likely

Looking at damage caused by people, effective Disaster Recovery Planning has even more benefits. Employees who are made aware of the importance of security can catch errors before they snowball into disasters; for example, an aware operations staff can actually stop a careless or untrained operator from entering the computer-equipment room with a donut balanced on top of a coffee cup. From personal experience, I can tell you that taking food into an area filled with delicate and expensive equipment is a really bad idea! In one case I recall, we spent days trying to figure out what was wrong with our mainframe tape drives. Eventually we found the culprit: some muffin crumbs that had been passed from tape-drive capstan to tape and back to tape drive. The ultimate culprit was someone in our operations staff, so I issued a stern directive that anyone caught eating or drinking in the machine room would be fired on the spot--and I also provided for alcohol towelettes to be placed at the entry to our operations room.

The point is that a small investment on the prevention side gave us far more benefit than just allowing the damage to continue and having our service contract provider absorb the costs of repair. The costs to us of downtime were far higher than the cost of the prevention measures.

Insurance companies recognize the value of prevention; consider for example the numerous

reductions of premium available for clients who install extra smoke detectors, heat detectors, fire extinguishers, breakage alarms, and direct connections to security firms. I just found out that our having installed a burglar alarm linked to a central monitoring station saved us 25% of our total premium. At that rate, our burglar alarm will pay for itself in just a few years. Finally, as Perry Bussom at the ICSA headquarters pointed out, if an insurance client doesn't have to claim damages at all, the premiums for regular insurance can go down--a hidden benefit of preventing and mitigating disasters.

On another level, security and disaster preparedness can make it less likely that an organization will be victimized by criminals. Well-protected organizations, like well-protected cars and homes, are less likely to be picked by professional crooks--it's just not worth the trouble when so many other easier victims are available. Similarly, an organization with a well-developed culture of security awareness is less likely to invite attack by dishonest employees or retaliation by disgruntled employees. So investing in Disaster Recovery Planning can actually reduce the risk of some kinds of human-mediated disasters.

Summary

In summary, Disaster Recovery Planning involves far more than figuring out how to react to a disaster. The spinoffs are manifold and valuable. Good planning to you!

M. E. Kabay is the Director of Education for the ICSA. If you enjoy his articles, you will want to order his new textbook,
The ICSA Guide to Enterprise Security: Protecting
Information Assets. McGraw-Hill (New York). ISBN 0-07-033147-2. 388 pp. Index.

Available from the ICSA Bookstore at 717-258-1816 ext 210