

Getting Your Disaster Recovery Plan Funded - with an Awesome Business Impact Analysis, Part 3



By [Leo Wrobel](#), [Sharon Wrobel](#)

Date: Jul 11, 2008

[Return to the article](#)

Leo and Sharon Wrobel conclude their three-part series with an example of the sort of helpful information available to businesses that are interested in relocating to exotic locations. (Or any location for that matter.) Organizations like the Pacific Disaster Center can provide the details to help you make the right decision

Last month we discussed the first two things that management positively needs to know in order to support and fund your disaster recovery planning effort

- What *can* happen? (Fire, flood, hurricane, sabotage, etc.)
- What is the *probability* that it will happen? (Expressed best in percent probability of the event in a given year.)

This month we conclude our discussion of techniques for securing approval and funding for your disaster recovery planning effort, discussing two more things that management positively needs to know

- What does it *cost* when it happens? (Think in terms of lost sales, market share, employee productivity and customer confidence.)
- What does *preventing* it cost? (Present a high-level overview of the proposed protective system, procedure, or function.)

Let's take up where we left off, with the *failure mode effects analysis* (FMEA). After showing where the FMEA fits into your executive presentation, we conclude with a couple more examples that speak specifically to the last two questions above that management *must* have answered before they endorse and fund your plan. Our hope is to impart some compelling tools that you can use to illustrate both of these issues, even to non-technical executives which can and *will* get your plan funded

Presentation Is Everything

Ask yourself this question: Where can you get the best food in the world? Probable answer: your mother's house. Your mom has lots of experience; the food tastes good; and, if you come from an Italian household like I do, the food is served in massive quantities. If I asked you to come and eat at my mom's house, however, you might be apprehensive. This is because you lack firsthand experience testifying that my mother is a great cook. In fact, you probably would be concerned about what you might get when you sit down to eat.

With those concerns in mind, where could we both agree to eat? What about the local French restaurant? With prices ranging upwards of \$300 for dinner for two, the food there had *better* be good. And the presentation is likely to be great, with beautiful plates of food and wonderful pizzazz. Not only will you not be apprehensive about eating at the French restaurant, you might even try something that you otherwise wouldn't eat (sils, for instance).

Disaster recovery can be looked at in much the same light. No matter how good your skills, management has no frame of reference that *proves* you're a good disaster recovery "chef." They're going to be apprehensive and skeptical of your cooking abilities. So what other option could you and your management team agree on today? The corollary to the French chef in this example is an expensive consultant. As with the French restaurant, management expects the consultant to be expensive, and expects that the product therefore will be good.

But is paying \$400 an hour for a consultant really in your organization's best interest? Will a consultant know your environment as well as you do? Will you even be able to claim ownership of the business resumption plan after the

consultant produces it for you? Notwithstanding the financial impact of such a project, these are some of the questions that you should be asking

It might be more advantageous to use some of the tricks of the trade that the expensive consultants use to communicate and sell their services. Let's consider some options for proving to management that you know how to cook up a good disaster recovery plan.

Management's Perception of Risk May Differ From Yours

Suppose 10 people in a room have identical incomes, bills, homes, cars, numbers of dependents, etc. Now ask those 10 people how much life insurance they should carry. You're likely to get 10 different answers. Some people are risk-averse and want the maximum amount of protection they can afford. Others want the least that they can get by with.

The same behaviors apply to decision-making executives. Since you probably won't know in advance how risk-averse your audience is, concentrate on presenting accurate probability data that spells out precisely how exposed your organization is to a catastrophic event.

How can you know the *probability* that a given piece of equipment will fail? This is why you have to be a technologist. You have a pretty good idea of the risks, but need to be able to communicate those risks to management in terms that they can understand. After all, management needs to know the probability of a failure in order to commit to funding your effort. They also need to understand *where* you got your figures in order to back them up with cash.

This is where the FMEA comes in, giving you a way to quantify the probability of a catastrophic failure in a piece of equipment or a system. I became familiar with this method in part from a conversation with a former U.S. Air Force general who was then the CIO of a \$75 billion financial services organization. Essentially, everything looking down at Iraq today from orbit was put up there by this guy's subordinates when he was still on active duty. He summed up the issue this way: "When we send up a military satellite, everything has to be perfect the first time. This is because no one has yet invented a 23,000-mile-long screwdriver to fix it."

I got the feeling from his tone that this was the voice of experience. Being a veteran myself, however (a sergeant, not a general), I could only imagine how many butts would be on the line if someone booted a \$100 million satellite launch. Therefore, in order to enhance the odds of getting it right the first time the military uses FMEA to compute the probability that something really pear-shaped might happen. It goes something like this:

1. Identify every mission-critical component that could fail
2. Compute or acquire from the manufacturer a *mean time between failure* (MTBF) figure for each identified mission-critical component.
3. Combine the failure probabilities into a single mathematical factor that describes the probability of failure of a given system.
4. Use these figures to justify and prioritize expenditures to "harden" equipment room, networks, or other facilities.

It's possible for corporate contingency planners to adapt this military FMEA methodology to our own uses. We adopted the Internet, right? As with many other aspects of recovery planning, here's another military invention we can dust off for commercial use.

Suppose you're tasked with performing a detailed analysis of your equipment room and associated networks. The objective of this analysis is to determine single points of failure, critical components that cause failures to multiple users, and an overall assessment of past performance or incidents. In order to describe this information, your FMEA will be broken down into three steps

1. **Identify the problem.** Determine what can possibly go wrong, including failure rates of the equipment itself as well as external factors (heat, water, air, people, etc.) that could affect it. Refer to the previous articles in this series for tips on how to complete this step.
2. **Assign a risk priority number (RPN) value for each of the issues identified in step 1.** (See [part 2](#) of this series for examples.) Use a number from 1 to 10, where the higher the number, the greater the associated risk (except in the case of problem resolution, where the higher the number, the better our speed in fixing the problem, as we'll show shortly)
3. **Quantify the reaction process.** Think "How fast can we fix the problem?" This step is shortened by

modifying your company's operating and security standards to moderate the risk and change the environment to make the selected systems more likely to survive. Here's a useful formula:

$$S \times O \times D = RPN$$

That is, *severity* (S) times *occurrence* (O) times *detection* (D) equals the risk priority number (RPN).

Once you have the "ingredients" you need to cook (in the form of the FMEA), you can borrow the "recipe" (presentation techniques) of an expensive French chef (consultant) to whip into something delicious that management will swallow and enjoy. A few techniques for doing this follow.

Visuals that Communicate Disaster Recovery Concepts

Good consultants make extensive use of pictures and graphs to communicate abstract concepts, since executives often have very little time to do a lot of reading. Use tools like the suggested matrix in Figure 1 to gather and organize your data into a format that can be understood and absorbed quickly by a busy executive.



Figure 1. Disaster prevention matrix

These steps help you fill in the blanks:

1. Start by considering each of the nasty things that could befall your organization (fire, flood, disgruntled employee, lightning, power failure, and so on). List each of these items (or perhaps just the top 20, based on the results of your FMEA) in the EVENT column. For example, list "Water in the equipment room."
2. Indicate the probability of the event. For example, what's the likelihood that a leak will occur in the equipment room? As we've stated in previous articles, you can't just dream up these figures. Consult reputable sources for credible information. For example, your organization's insurance provider undoubtedly has actuarial tables for such disasters.
3. List the potential cost of the event. Assemble your figures from estimates provided by corporate staff and other people. For example, the VP of sales may have a commission incentive plan based on sales, and would be able to venture a reasonable estimate of lost sales due to equipment outage.
4. Project how long the disaster would disrupt operations (1/2 day, three days, seven days? Management will automatically multiply the cost figure in the previous column by the time figure. This is by design. Rather than concentrating on the technology, management concentrates on the money. This is how it should be, and how it *will* be if you do a good job at substantiating your figures.
5. Specify the money that you'll need in order to prevent or alleviate the problem. Nice that management can make a decision here *without* concentrating on the technology. It's possible that management won't even understand what equipment you're requesting. If you need fire extinguishers for the equipment room, that's one thing. But what if you're asking for route diversity on a dual-fed counter-rotating fiber-optic ring from the telco? Your management team probably won't know what that is but referring back to the EVENT column, they'll see that you've listed "Telephone cable cut." That's enough information to make a decision.
6. Finally, since you'll be asking for a lot of money in many different forms, indicate the financial benefit or the priority for each item. This helps everyone to understand that the lack of a fire prevention system in the equipment room is a higher priority than, for example, the failure of a small network workgroup.

Now that you've gone through this example, albeit a very modest example, ask yourself how the proposal to your executives would have gone if you just asked for money skipping the other essential information! Yet this is exactly what many technologists do year after year, not because they don't know what they need but because they don't know how to communicate that need effectively to management, in terms that management can understand.

Assembling Your Tools

Almost without exception, the slides and communications mediums we're suggesting speak to *business* issues and not *technical* issues. Business terminology is the topic in which executives are conversant not technology issues. A good consultant always writes for his audience

The following lists pull together the most important concepts and suggestions to take from this series:

Sources of probability data:

- Personal experience
- Experience of your organization
- Experience of others
- Research
- Trade groups
- Insurance companies/actuarial tables
- National Fire Protection Association (NFPA), Federal Emergency Management Agency (FEMA), National Weather Service (NWS), other agencies

Presenting the probability of a disaster:

- Figures must be substantiated.
- Figures must be relevant to your organization
- Best expressed in percentage probability.
- Figures must communicate *easily*. (Use color, charts, graphs, if possible.)
- Consider conducting a failure mode effects analysis (FMEA)

Characteristics of a good presentation:

- Brief, 30-40 slides. Use good visual media
- Well-researched materials and figures
- Validated with persons that executives trust
- Uses terms that executives understand
- Covers the four things that executives need to know
 - What *can* happen?
 - What is the *probability* that it will happen?
 - What does it *cost* when it happens?
 - What does *preventing* it cost?
- Conclusions substantiated with people that management trusts
 - Corporate controller or CFO
 - General counsel
 - Vice president of sales, marketing, production, MIS, technical services, etc
 - Subsidiary/corporate officers

Summary

We hope that these examples will jog a few ideas loose for you on how to present a compelling funding request to executive management. By establishing "hard" and substantiated probabilities, backed by individuals whom management trusts, *it may not even be necessary* that management understand precisely the technical capability of the equipment you propose! It's more important that they clearly understand the business risk your proposed solution alleviates, so that they can make informed decisions. The comfort level you establish with management in this regard translates directly into approval of purchases, project funding, and general support.

If you follow the rules in this series, we are confident that you will convince your management that you too can be a master chef, and that they can safely swallow anything you cook up in the way of disaster recovery. Best of luck in your pursuits!

NOTE

There's a lot more to a successful executive presentation than we've had space to address in these three brief articles. For more suggestions, see my book *Business Resumption Planning, Second Edition* (Taylor Publishing 2008).

Leo A. Wrobel has more than 30 years of experience with a host of firms engaged in banking, manufacturing, telecommunications services, and government. An active author and technical futurist, he has published 10 books and more than 400 trade articles on a wide variety of technical subjects. Leo served 10 years as an elected mayor and city councilman (but says he is better now). A sought-after speaker, he has lectured throughout the United States and overseas and has appeared on several television news programs. Leo is presently CEO of Dallas-based TelLAWCom Labs Inc. and b4Ci, Inc. Contact Leo at 214-888-1300 or email leo@b4ci.com.

Sharon M. (Ford) Wrobel served as corporate secretary and director of personnel for Premiere Network Services Inc. prior to joining b4Ci, Inc. in 2004. During that time, Sharon was instrumental in getting Premiere certified as the first CLEC to be certified in all 50 states, by aiding in filings and attending hearings. She also engaged in extensive research for Premiere, a function she continues with b4Ci as vice president of business development. Sharon was also president of the Ellis County Early Childhood PTA and the Ovilla Lions Club. She attended the University of Maryland and El Centro College in Dallas and received training as a registered nurse before joining Leo in business in the late 1990s. Sharon also served as a public official by accepting appointments to the local Planning and Zoning Commission and the Historical Commission.
