

BY LEO A. WROBEL

Common Mistakes in Business Resumption Planning: Part II

Understanding the mission of the technical systems that support your organization and their vulnerabilities is critical to developing a sound Failure Mode Effects Analysis, the second step in creating a Business Resumption Plan.

In Part I (*Technical Support*, October 1997) we spent a significant amount of time on the need for a well-done Business Impact Analysis (BIA). This month as promised, we will take a more technical slant to the topic as we discuss the second most common mistake in Business Resumption Planning: shortcutting or skipping the FMEA (Failure Mode Effects Analysis), which is the supporting data not for the business dynamics, as we discussed last month, but for the technical systems which support the business. A reliable FMEA is the second major step toward a successful Business Resumption Plan.

CONDUCTING A FAILURE MODE EFFECTS ANALYSIS (FMEA)

The CIO of a \$25 billion organization, who was also an ex-Air Force general and telecommunications officer, once commented to me, “When we send up a military satellite, everything has to be perfect. Everything. This is because no one has yet invented a 23,000 mile long screwdriver to fix it if it is not [perfect].”

I got the feeling this was the voice of experience, but did not broach the subject any further. Because “everything has to be perfect,” the military is particularly fond of Failure Mode Effects Analysis – indeed, FMEA originated with the U.S. military. Find everything that can go wrong, evaluate the MTBF (mean time between failure) for each component, then combine them into a single mathematical factor that describes the probability of failure of the system as a whole. It’s not easy, but we can adapt a similar methodology to our work as contingency planners in the corporate world, then use it as a guide when setting standards.

Here’s how:

Suppose you are tasked with performing a detailed analysis of the installed backbone network and the related equipment attached to the backbone. The objective of this analysis is to determine single points of failure, critical components that cause failures to multiple users, and provide an overall assessment of past performance of these devices. The following information outlines the methodology you can use to accomplish this.

COMPONENTS OF AN FMEA

An FMEA is broken down into three components: The first is the Problem Identification step. When designing or evaluating a network both in hardware and software, the rule-of-thumb is to ask, “What can possibly go wrong?” This includes both failure rates of the equipment itself as well as the external factors (heat, water, air, people, etc.) that could affect it.

The second component is the assignment of a Risk Priority Number (RPN) to each of the probabilities. Pick a number from one to 10. The higher the number, the greater the associated risk. In the case of problem resolution, the higher number indicates a longer time to detect and correct the problem.

The third and final component is Standards Refinement, or the development of a reaction planning process. This is the “How fast can we fix the problem?” step. This is best done by modifying your company’s Operating and Security Standards to moderate the risk and change the environment to make the selected system more survivable.

CALCULATING RISK PRIORITY NUMBERS (RPNS)

Failure rates are then assigned from the probability based on statistical and historical

The objective of this analysis is to determine single points of failure, critical components that cause failures to multiple users, and provide an overall assessment of past performance of these devices.

data accumulated over the past from manufacturers' data or other sources. Then, three factors are considered and weighted:

- ◆ Severity
- ◆ Frequency
- ◆ Detection

Severity is assigned a numerical value from one to 10 (the higher the number, the more severe) based on the probability of an event, and how damaging it would be.

Frequency of the occurrences by part type is similarly assigned a value based on how often you expect it to happen (the higher the number, the greater the frequency of occurrence).

Lastly, difficulty of *detection* and repair is weighted so that the higher the number, the more difficult the problem is to detect and fix.

These three factors are multiplied together to form the RPN, which is used to assist the team in assigning priorities to address or assess higher priority treatment on specific elements. This is not a qualifier/disqualifier but a determination of what can and will go wrong. From there, resources (capital or human) can be assigned to minimize the risks associated with these areas. The issues with the highest RPNs are the areas where your organization is most vulnerable and needs to spend the most time and resources.

Severity Rating

When a component on the network fails, the severity is classified in a 10-point system as shown in the table in Figure 1. A single point of failure, for instance, could be the backbone network. Many components make up this single point of failure, including such things as the building environmental conditions, or the building and closet entrance facilities for the cabling and the

Figure 1: 10-Point System to Classify Severity of an Outage

Description	Rating
If one user is affected	1
If a workgroup is affected	2
If an entire bay is affected	4
If a single floor is affected	6
If an entire building is affected	8
If the entire backbone is affected	10

Figure 2: Frequency of an Event

Occurrence Level or Frequency	Rating
If every day	10
Weekly intervals	8
Monthly intervals	6
Quarterly intervals	4
Every 12 months or longer	2

power. These would have a severity rating of 10 if they were to fail, even though the building was still intact.

Occurrences

If a failure occurs often enough, the frequency of an event is a concern regardless of the severity. See Figure 2. If the failures occur continually or manifest themselves on a daily basis, then the critical rating here is the highest.

Detection/Repair of the Failure

The easier it is to detect the problem and begin corrective measures, the lower the critical rating; conversely, the longer it takes, the higher the rating. See Figure 3.

Risk Priority Numbers (RPNs)

Based on the factors of security, occurrences and detection, the mathematical computation for RPN is:

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

$$10 \times 10 \times 10 = 1000$$

The higher the RPN; the higher the risk associated with a specific component and the higher the value that would be placed on

solving the problem. If a network is comprised of several critical components that have very high RPNs, it is necessary to determine where the network can be improved to support the expected service levels.

STANDARDS REFINEMENT

The final component is the Standards Refinement step, or the "What are we going to do about it?" step. Ongoing maintenance and repair procedures should be designed to prevent disasters before they happen in the first place. Change control and management control over a system are even more important. When properly orchestrated, however, standards pay off handsomely in reduced operating costs as well as in greater peace of mind which comes with a more robust operating environment.

The following presents some tips for evaluating the physical environment as part of the FMEA component of the study.

BASIC PHYSICAL STANDARDS FOR ALL INSTALLATIONS

It is no longer necessary to physically differentiate among different types of equipment installations. Telecommunications switches act like (rather they are) large

computers and deserve the same protection as mainframes. Mainframes generally don't require the excess baggage of years past (chilling water, 400Hz power, etc.), so they can sustain themselves in a well conditioned space, not necessarily an "environment."

For many companies LANs are taking the place of mainframes, and mission-critical applications are migrating to these boxes on a daily basis. As such, the standards that used to apply to the mainframe, should apply to the LAN server now. This includes such things as:

Access to computer rooms: Who can get in and out? How many times in your organization does the telecommunications department make a change on an important server, followed 10 minutes later by the LAN department, and then later in the day by the mainframe guys. Then the system crashes and, of course, it is nobody's fault! How about a sign-in log and procedure to track these inter-departmental changes?

Access to visitors: Here's a true story: A woman who was an IS manager went into the office on her day off to check a few pressing matters. She took her five-year old son along. After being repeatedly assured by her staff that everything was under control (and also chided for not enjoying her day off) she took her eyes off her son for just a moment. The key for the main UPS, about 12 inches from floor level, proved irresistible to the little guy and ... (need I finish with the gory details?) Needless to say, she still works for the company, but doesn't this make my point?

Additional physical protection: Many LAN environments are installed where nobody ever had any business installing equipment: basements, closets, other locations. How is the air flow in that cramped closet that is now your server room? Do the doors lock? Is the janitor in there? Would you feel better if those big glass windows in your server area or computer room were not glass?

Other building improvements: How is your general building condition and security? Power? Access? Age?

Remote system access: Have you checked your controls for remote access lately?

Figure 3: Critical Rating Based on Timeframe for Detection/Repair

Description/ Detection	Rating
Is easy and resolution can be achieved within one hour	2
Greater than one hour but less than four hours	4
Greater than four hours but less than eight hours	6
Greater than eight but less than 24 hours	8
Greater than 24 hours	10

How much confidential information could be leaving your organization this instant on a \$79 fax modem on someone's workstation — perhaps a modem you are not even aware of is installed!

Just as in mainframes and LANs, it is important to establish a protocol and procedure for not introducing new applications directly into a production environment.

Controls for remote access: Who do you allow remote system access, and at what level of security? Everybody? Unlimited? You are asking for it!

Housekeeping: Do you store large piles of paper or combustibles in your server area? Do you ban smoking? Pop a floor tile and look under it.

Electrical power: Spikes, shorts, brownouts, blackouts and sags. Many buildings were wired long before clean power was a consideration. Do you take adequate precautions with mission-critical equipment now? UPSes are inexpensive and will save you many problems.

Fire protective systems: Don't try to be the expert, bring one in for a survey.

ASSESSING CHANGE CONTROL PROCEDURES

What's the most common cause of disasters? Probably people. You can control them through your Standards and Change Management procedures. Here's how:

Network software security and change control management: Every technical system (LANs and mainframes) should have a formal and documented change control system that defines, but is not limited to, the following:

- ◆ major software changes
- ◆ persons authorized to make changes
- ◆ password protection of maintenance functions
- ◆ back up during software changes

Backup -48V power for telecommunications equipment: When evaluating telecommunications systems one of the most critical items to consider is the lack of some type of -48 volt backup station power for the DACS (Digital Access Crossconnect Systems), SONET and lightguide transmission equipment, and other telecommunications equipment. Many companies have crossed the invisible boundary between being a large corporate user and being a central office service provider. As such, the organization is on a learning curve as to which standards and procedures apply to prudent operation of a central office environment. A set of standards for backup power is one of these concerns.

Another way of looking at it would be to picture a room full of doctors trying to save a patient's kidneys after his heart had stopped beating. All other recovery activities would pale in significance to a failure in this area.

The fiber optic lightguide termination equipment is the heart of many communications-intensive businesses. It forms the fundamental layer of raw transport on which all other systems are built. For example, if this equipment includes a -48 volt battery backup, your technical personnel will have an additional eight to 16 hours of "forgiveness" while isolating

problems on, say, the UPS bus or in other cases of major failure. However, don't assume your UPS will be enough — they fail, too. Phone companies use batteries and so should you. The need to install a backup -48 volt power supply for critical-transmission equipment, an accepted and common practice in central office locations, cannot be overstated.

Internet Concerns

Who is responsible for Internet security? Many organizations still have some unresolved organizational issues with regard to security responsibilities for the Internet. Historically, these types of operations may have fallen under a mainframe or mid-range computer group in the IS department. Other departments may have separate groups of technologists responsible for the actual operation of the Internet firewall and other components. They may reside in data security, LAN operations or other departments.

Snafus (i.e., holes or vulnerabilities left temporarily exposed in the system) may occur due to the lack of a clear-cut policy outlining exactly who is responsible for which system and under what circumstances. While ultimate responsibility could gravitate by default to a mainframe or mid-range computer group, this function should be closely monitored by a security group, at least until the technology matures. Your company should also consider a nominal increase in manpower to provide depth and avoid creating too small a pool of "specialists." Once the company has its feet wet with regard to Internet access and is confident that any possible security breeches or holes are closed, organization changes may be readdressed.

INSTALLATION OF A TEST FIREWALL

My company has noticed in past analysis of physical components comprising

corporate firewalls that there is usually no firewall platform exclusively earmarked for testing and back up. For all intents and purposes, the present technology is single-threaded in almost every way. This is not a major concern yet, but it will be when your company's firewall goes into revenue-impacting mode, assuming it has not already.


Another concern is network diversity. Often there is only one T1 to the ISP (Internet Service Provider) which, again, creates a single point of vulnerability.

Just as in mainframes and LANs, it is important to establish a protocol and procedure for not introducing new applications directly into a production environment. Secondly, a test firewall can also double as a backup in the event of a major equipment failure in the primary. Finally, because the Internet is a relatively new technology for many organizations, the staff should be encouraged to dabble. It would not be considered prudent practice to experiment on a production platform.

Hardware upgrades are also often in order. Many of the routers commonly in use today have no redundancy. The Cisco 5000 series, for example, has redundant power and a redundant CPU. Another concern is network diversity. Often there is only one T1 to the ISP (Internet Service Provider) which, again, creates a single point of vulnerability. A second T1 should be added along with "Round Robin DNS" for greater resiliency on the WAN connectivity to the ISP. Other components, such as CSUs and

DSUs are often single-threaded with no redundancy. Check the status of these items if Internet access for your company is a revenue-impacting application.

SUMMARY

Armed with the information from Part I and this month's discussion of the FMEA, you should be well on your way to understanding the mission of the technical systems that support your organization and some of their unique vulnerabilities. Part III will build further on this knowledge by examining some of the most common mistakes in writing the Business Resumption Plan itself. Stay tuned, and good luck! 



Portions of this article were adapted from Leo A. Wrobel's books *Business Resumption Planning* (third update © 1997 Auerbach Publishers) and *The Definitive Guide to Business Resumption Planning* (© 1997 Artech House Books, Norwood, MA). Reprinted with Permission. Wrobel has eight other titles in print and more than 20 years experience in all phases of information technology. For information on Wrobel's books, or the 12-year old management consultancy of which he is president and CEO, contact his web site at www.dallas.net/~premiere or call (972) 515-5000.

©1997 Technical Enterprises, Inc. Reprinted with permission of *Technical Support* magazine. For subscription information, email mbrship@naspa.net or call 414-768-8000, Ext. 116.