

Risk Analysis Made Easy

By Robert V. Jacobson CISSP

In an effort to make operational risk analysis easy, a number of writers have proposed a matrix of risks ranked as Low, Medium, and High, and loss exposures, also ranging from Low to High. This certainly couldn't be much easier, but the typical 1,000 word blurb in a magazine article is too short to give enough attention to the details. However, attentive readers of these "Risk Analysis Made Easy" articles sense that something is not quite right. It's the lack of details and meaningful examples that causes the uneasiness. At the risk of being a killjoy, let's look at some of the details.

At first glance Low, Medium, and High appear to neatly sidestep the problem of quantification. Let's see if the promise can be fulfilled. If we operate a Web store selling clothing, how shall we rank the threat: Hacker Website Attack (HWA)? Well, we all agree that this is a major threat, so we will rank it as High. How about Denial of Service Attack (DSA)? Since a HWA could result in a disclosure of customer credit card numbers that could put us out of business, it seems more threatening than DSA, which only results in the loss of some sales revenue. We will rank DSA as Medium. Next, how shall we rank Electric Power Failure (EPF)? We have a 30-minute UPS, but the blackout in August 2003 lasted forty-eight hours in some locations. That would be much worse than a typical DSA, but not as bad as a HWA. So, do we rank EPF as Medium or High? The more threats we consider, the more difficult it becomes to fit them all into one of the three categories simply is not realistic, and it is not unusual to find that a risk analysis includes 25 or more threats.

Here is another issue. We have both Web Sales and Catalog Sales. Catalog Sales account for 30% of our revenue, and Web Sales the other 70%. So we rank the two business processes thusly: Catalog Sales as Medium, and Web Sales as High. This means that Web Sales-DSA is a High-Medium risk, and Catalog Sales-HWA is a Medium-High risk. Wait a minute! Catalog sales are not vulnerable to HWA, so this should be a zero risk! Furthermore, we realize that Catalog Sales are less vulnerable to EPF than are Web Sales. The vulnerability is not zero, but it isn't 100% either. It becomes clear that we need another factor: the Vulnerability of each of our business processes to each of our threats.

Bearing in mind that we are performing this risk analysis to decide where to spend limited resources to manage our risks, it has become clear that our simple 3 x 3 matrix is just not going to work for three basic reasons. First, it does not provide enough granularity to express the full range of differences among threats, and among loss exposures. Second, we realize that not all loss exposures are vulnerable to all threats. Finally, identifying a High-High risk, a Medium-High risk, a High-Medium risks, a Low-High risk, etc., etc. just doesn't tell us how to allocate our limited resources among the risks, or even if the amount allocated to risk management is optimum.

We can resolve the first two deficiencies if we abandon Low-Medium-High, and use numerical scales for threat occurrence rates, business process loss exposures, and vulnerability factors. Specifically, we will estimate the number of occurrences per year of the threats, the potential monetary loss of each of our business processes in dollars per threat impact, and the vulnerability, zero to 100%, of each process to each threat. Note that we will assume an impact of the worst-case threat when we estimate loss potential. This quantified model will be much more satisfying because now we can evaluate each risk (a threat vs. a loss exposure) in terms of dollars of expected loss like this::

$$\begin{aligned} \text{Expected Loss (\$/year)} &= \text{Threat occurrence rate (\#/year)} \\ &\quad \times \text{Process Loss Potential (\$/occurrence)} \\ &\quad \times \text{Vulnerability Factor (0.0 to 1.0)} \end{aligned}$$

This is certainly a much more accurate loss model than High-Low, and so some writers have proposed this model. However, there is yet another issue we must address. Assume that we have two business processes, A and B, with the same loss potential parameters. Assume further that A runs 24x7, but that B only runs for two hours once a week. If we keep score for a year, will we find that since they have the same loss potential, they have had the same total loss experience? Clearly not even though they have the same loss rate. B will miss most of the short duration service interruptions while A will be impacted by all of the interruptions. Obviously, we must adjust our expected loss equation to take into account the slack time between scheduled operations of each process.

Here is another complication. In the example just above, we have assumed a linear loss mechanism for the two processes, \$1,000/hour. However, if we interview the line of business managers we may find a much more complicated situation. For example one manager may say that there is no significant loss for his business process unless the service interruption lasts for at least two hours, but that after the second day of an interruption, the hourly loss rate doubles. The manager of a billing system would point out that the interest lost when revenue is delayed (the time-value of money) is very definitely nonlinear, and mentions something called a Fibonacci series as the basic loss mechanism.

If the loss potential rates of business processes are not linear, this means that we must take into account the duration of the service interruptions that each of the threats will cause. However, a little reflection shows us that a given threat, for example Electric Power Failure will cause a range of outage durations. If all loss potentials were linear, and losses always began at the beginning of each service interruption, we could probably use an average outage duration for each of the threats, but now we know that this is not the case. While we would like to keep our risk analysis simple, is it not more important that our model leads to accurate estimates of loss? This means that we must define a profile of outage durations for each of our threats, use accurate business process loss potential rates, allow for differences in vulnerability, and make appropriate adjustments for slack times.

If this weren't enough, we will discover more complications when we attempt to cost-justify risk management measures. It is relatively easy to estimate the cost to install and maintain a proposed measure, estimating its benefit is more difficult. This is because a given measure may affect more than one threat in any one or more of three ways. A measure may reduce a threat's occurrence rate or its outage duration profile, and it may reduce or increase the vulnerability of one or more of the business processes to one or more of the threats. To evaluate the Return On Investment (ROI) of a proposed measure, we must make all of the required adjustments to the parameters on the threats affected by the measure, and then recalculate Expected Loss to determine the *reduction* in Expected Loss that we can expect the measure to yield. This reduction is the Return, and the present value of the cost to install and maintain is the Investment. Knowing these two factors, we can calculate the ROI for each proposed measure.

Unfortunately, there is one final complication. When we consider the simultaneous application of two or more risk management measures, each of which presumably has a favorable ROI, we can't simply add the individual reductions in expected loss. This could result in negative expected loss, clearly an unrealistic result. What we must do is estimate the *collective* effect of a group of risk management measures on the threats since some of the effects may be overlapping. For example, this can easily be the case when we consider several different kinds of internal controls applied to the same business process.

We have failed miserably in our attempt to make operational risk analysis easy, but we have identified the components required of a risk model to take into account the basic factors that determine expected loss. Here are the factors we have identified:

- Quantitative estimates of risk parameters, not Low-Medium-High, are required because of the wide range of values we will encounter in the real world.
- Non-linear business process loss mechanisms block the use of a simple fixed hourly rate.
- Threat outage duration profiles are required because of the non-linearity of the loss potentials.
- Vulnerability factors ranging from zero to 100% are required to correctly model the interactions between threats and business processes and assets.
- Scheduling slack time modifies expected loss.
- Complex interaction between threats and risk management measures.
- Potentially duplicative effects of risk management measures.

Furthermore, it is clear that we must make many estimates of expected loss during the course of a risk analysis project. This means that we must have an automated tool to store and collate the input data, perform the complex calculation, and then display the results in a meaningful form.

Why have we failed to find an easy way to do risk analyses? Not because we didn't try hard enough. The reason is self-evident. *Risk is complicated*. Simplistic Low-Medium-High loss models are simply incapable of yielding trustworthy results. Is it

important to assess risk accurately? With the onset of the Industrial Revolution, the world got more complicated, and this complexity has increased exponentially. Recent history is replete with examples of the failure of guesswork as a risk management technique. The recent hundred-year flood of the Mississippi, the major forest fires in California, the August 2003 eastern blackout, and failed commercial Web sites are striking examples of failures to assess risks accurately. Compliance with Sarbanes-Oxley, Basel II and other similar regulations add another essential reason for accurate risk assessment and management.

CORA[®], International Security Technology's Cost-of-Risk Analysis system, implements a complex mathematical model of the risk factors described above (and a few more too complex for this short description) to ensure that its estimates of expected loss are valid. In short **CORA** is complicated because risk is complicated. Because it is automated, **CORA** makes it easy to repeat a risk analysis as often as necessary to validate the input data. However, when first confronted with **CORA** it is not uncommon for a user to express concern about its complexity. Indeed, recently a user remarked that: "**CORA** has too many buttons." However, all those buttons are the key to unlocking the mysteries of risk loss exposures, and to ensure that due care, not guesswork, has been used to analyze risks, and select optimum risk management strategies.