Why Information Systems and Business Continuity Must Dovetail

By Brian Davey

When analyzing threats to an organization, we need to calculate the risk each threat poses.

The problem with probability

We know that when analyzing threats to an organization, we need to calculate the risk each threat poses. Risk is composed of two elements – probability and impact. The negative impacts which would result from a threat materializing can be determined fairly accurately through a process such as the business impact analysis, or BIA, generally employed as part of a business continuity management (BCM) program. Negative impacts such as loss of revenue, lost business opportunity, breach of legislation and/or regulation, customer dissatisfaction, negative brand impact, loss of market share, etc., can be explored with the appropriate business representatives, to arrive at a likely cost to the organization should the threat materialize.

Based on the risk score, the organization then usually agrees upon a course of action to manage the threat, that is, to either accept, transfer, treat or avoid the risk. The problem is that the scoring of probability is inherently flawed.

Let me explain. How high would you rate the probability of your home being broken into? You may say that the probability is very low, given your low-crime neighbourhood, security locks, burglar alarm and a history of no burglaries in your street in the last ten years.

Now what if you know that a professional burglar has just rented the house next door to you and has taken a liking to the expensive home entertainment system he has caught sight of through your window? I would guess that the probability rating has just moved up a notch or two.

If we had put the world's top 100 risk managers in a room on September 10, 2001 and asked them to rate the probability of the twin towers being destroyed with around 3,000 lives lost within the next 24 hours, how many of them would have said, "The likelihood rating is off the top of the scale – in fact it's a sure thing"?

How many times have fraud investigators heard a remark along the lines of, "I would never have believed that Fred could have stolen money from the firm. He always seemed such a nice chap"? Many times, is the answer.

Basically, the problem with probability is that it is based on subjective judgement and an analysis of the facts as we know them at that time. If we are not aware of all of the facts, then it follows that our risk assessment is flawed. Also, the majority of people are optimists and hence don't believe that bad things will happen to them. This view transfers to the organizational setting as well. In my experience, senior management teams seem to have endless optimism, as they need to in order to overcome hurdles, keep the company moving forward, and beat the competition.

Ask yourself the following question, and answer it honestly. The fact that a serious security threat to the organization hasn't materialized so far is down to:

a) Sound management and controls

b) Luck

c) We haven't been targeted as yet

Assume the worst, and plan for it

So what am I getting at? Well, the way I see it, we always need to assume the worst-case scenario, that is, that the threat will materialize no matter how ultra-low we may think the probability is. Hence, if we have calculated for any threat that the resultant negative impacts on the organization would be at an unacceptable level, then we need to plan for just such a situation arising. Otherwise we are not discharging our duty as threat managers with responsibility for trying to keep the organization safe from harm.

Business continuity plans should not just cover the traditional fire, flood or explosion types of threats. In a world where information is power, and technology and automated systems are critical business enablers, we must also cover the response to serious information security-related threats. Regardless of the controls we have in place to protect the organization from physical or virtual security threats, we must also have an agreed fall-back plan to invoke should a threat materialize.

In other words, we need information security controls to try and prevent the serious breaches, but we must also have a business continuity plan, including technology and systems recovery, which will provide us with a fall-back strategy, response, and recovery back to a business-as-usual state, should a serious breach occur. IS and BC must dovetail.

If your organization has a business continuity plan, including the requisite response teams and escalation process underpinning it, is the plan flexible enough to cover an information security threat materializing? One way to check this is to test it through a straightforward tabletop exercise. Get the primary response team in a meeting room and provide them with a scenario to manage, such as:

- You have just been informed that our main competitors have a copy of our confidential business plans
- A new virus has just got through our defenses and is running loose on our network
- An employee has just confessed to embezzling £500,000 from the company over the last five years

Each of these scenarios requires not just an initial response to investigate and contain the situation, but will also require effective stakeholder communication and possibly damage limitation. These areas demand senior management-level involvement and decision-making, plus input from subject specialists such as Human Resources, Legal, and Public Relations. A well-prepared business continuity plan should already cover the senior management and expert involvement required for these scenarios.

Such an exercise will help to expose whether or not the business continuity plan is appropriate to handle the materialization of threats to information security. The plan should also test whether an escalation process exists, and if it is appropriate to serious information security breaches. If it isn't, then can I be so bold as to suggest that you update it, as a priority? After all, you never really know what the true probability is that a serious breach will occur very, very soon. Do you?

About the Author

Brian Davey is Senior Consultant at Teed Business Continuity, which will exhibit at Business Continuity – The Risk Management Expo 2007.