

**Topic:**  
Business  
Continuity

## Business Continuity Management

**Ask yourself the following question and answer it honestly ...**

**“The fact that a serious security threat to the organisation hasn’t materialised so far is down to:**

- a) sound management and controls?**
- b) luck?; or**
- c) we haven’t been targeted as yet?”**

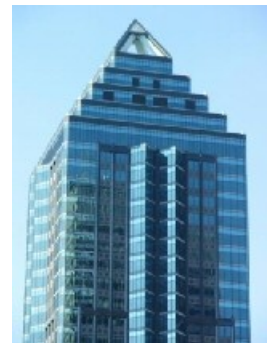
*iCT is produced by Business Advantage, a B2B research, business development and marketing consulting practice operating in the global IT, Digital and Telecommunication sectors.*

### Why Information Systems and Business Continuity Must Dovetail

#### *The Problem with Probability*

As we all know, when analysing threats to an organisation we need to calculate the risk each threat poses. Risk is comprised of two elements – probability and impact.

The negative impacts which would result from a threat materialising 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 programme. 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 relevant business representatives to arrive at a likely cost to the organisation should the threat materialise.



Based on the risk score the organisation then usually agrees the course of action to manage the threat i.e. to 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 history of no burglaries in your street in the last ten years.

Now what if I say to you that a professional burglar has just rented the house next door to you and add that he 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 10th September, 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”?

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 organisational 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 organisation hasn't materialised so far is down to a) sound management and controls, b) luck or c) we haven't been targeted as yet.”

*Assume the worst will happen 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 i.e. that the threat will materialise no matter how ultra low we may think the probability is. Hence if we have calculated that for any threat where the resultant negative impacts on the organisation 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 organisation safe from harm.

Business continuity plans should not just cover the traditional fire, flood, explosion type 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 organisation from physical or virtual security threats we must also have an agreed fallback plan to invoke should a threat materialise. 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 fallback strategy, response and recovery back to “business as usual” state should a serious breach occur. IS and BC must dovetail.

If your organisation 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 materialising? 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” or “A new virus has just got through our defences and is running loose on our network” or “An employee has just confessed to embezzling £500,000 from the company over the last 5 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, areas which demand senior management level involvement and decision making plus input from subject specialists such as HR, Legal, PR etc. 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 understand whether or not the business continuity plan is appropriate to handle information security related threats materialising. The plan should also test that an escalation process exists and 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?**

*This article was contributed by Brian Davey – Senior Consultant at Teed Business Continuity. Please [Click HERE](#) to leave a comment or question.*