# 2007-07
# Making Better Security Decisions

## Introduction:

It would sure be nice if we could make better strategic decisions about security. But how exactly do we do this? Despite efforts over several decades, decisions of today about security are much like those of long ago. They are highly dependent on the individuals making them and the specific circumstances.

## Over-think vs. under-think

One of the major complaints I hear from those who know a great deal about information protection is that management and pundits don't have a clue about the scope and complexity of the issues in security. I agree with them on this. Most non-experts under-think the issues of security. But I think it should also be said that many in the security industry also over-think the issues from a standpoint of the context in which they are made.

Somewhere in the middle – between the expert who spends day and night obsessing over what are in deed trivialities from the standpoint of the enterprise, even if they are substantive with regard to their particular focus – and the executive who really just wants security to go away as a problem but keeps getting dinged by it – there is a sensible middle ground that we need to find.

## Where is the middle?

If there is a middle ground, where is it and how do we find it? Our view, and the view of many others in the field, is that the middle ground lies somewhere near the field of risk management. But this must be expressed with some caution and a lot of trepidation. Risk analysis is one of the most poorly understood and worst practiced areas of information security today, and it is often confused with risk management. Metrics for risk management are poor at best, and management loves metrics because, as the saying goes, “you can't manage what you can't measure”.

But of course this is far from the truth. You can in deed manage what you cannot measure – or perhaps more to the point – you can find a way to measure anything for the purposes of managing it. The challenge is to find the measurements that are meaningful to management and codify decisions in those terms.

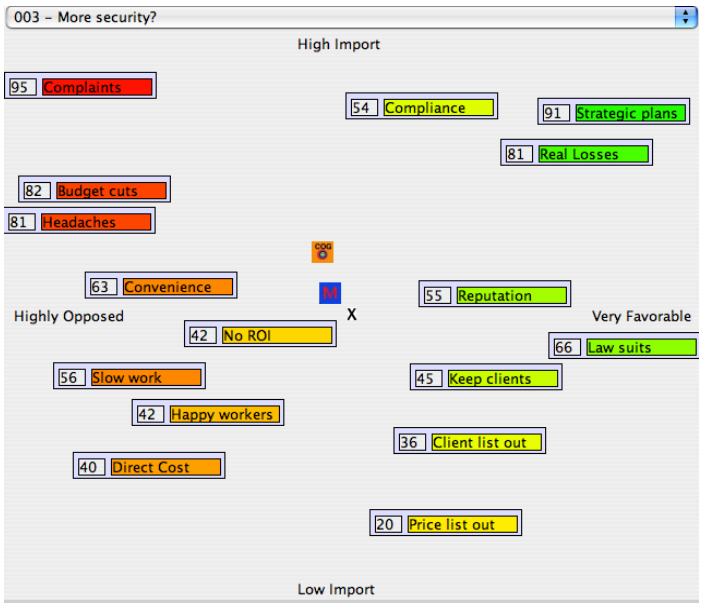
The middle ground is in the mind of the decision-maker.

## How do I get into their head?

Getting into the mind of the decision-maker is the job of every information security manager and executive. But how do you do it?

We have an approach for this, but it gets tricky when we are outsiders and don't have a long time to get at the information. We tend to do it through a group process, or if we can get such an appointment, through an individual meeting.

In the meeting, we start by asking the decision-maker (DM) what they think is important to information security from a standpoint of the overall company. We used to do this with a series of questions and discussions, but it sounded to most DMs like they were defendants in a legal matter. Now we do it with a decision support tool that takes their views and puts them on a display – right in front of them – and allows them to identify what's how important to them, and what acts for and against having more or less protection in their minds.




We start with their ideas and then, as they run low, we add in some of the other ideas from our library of factors in the decision. As they see the issues forming in front of them, they decide what is how important to them, and we add notes on the details behind their views.

## Conclusions:

Making better security decisions starts with understanding the key factors in the minds of the decision-makers. From there, priorities can be set and focus laid on what's important to them.

## Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 57, section 2.7.1.3 we present the every popular:

**"Help me get the money out"**

> *"It's 100% risk free! Make millions for almost nothing! ... All you need to do is..."*

Whoever it is that has millions and millions of dollars in some foreign currency desperately needs your help to get the money out. It's illegal there – but it's just! Or it's legal but unseemly... or whatever... it's all the same. Only you out of the whole world can help them get the millions out – and they will reward you handsomely for it. As if...

Section 6.3.1.1.3 (page 184), "I miss golden opportunities – on purpose" tells us:

> *"Will I miss a golden opportunity some day? Sure I might, but I will also miss all the rotten opportunities to get ripped off..."*

Unless you want to lose what you work so hard for, you will have to look lots of Internet-based gift horses in the mouth. No matter how plausible it sounds that you could make millions by doing nothing, except for high ranking political figures who can break the law with impunity, don't imagine that anybody will give you millions of dollars because they picked you out of the Internet to help them.

## Chet's Corner

I am convinced that management doesn't care at all about information security. They don't want to know about it, they don't want to pay for it, they don't want to do it, and they will only spent time or money on it if they are forced to, and then they will find a way to get back at those who forced them to do it. When it comes to budget cuts, they will fire the information security executives and staff in a heart beat because they can't prove their worth... which is why it pays to be a consultant. After all, when it hits the fan, they can't really call back the security managers they just fired...

"Always look on the bright side of life"!

## Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's strategic scenario experiences.

There is a long history of the use of scenario experiences (sometimes called games) used to help identify and prioritize issues within specific contexts. This has ultimately led to a wide array of different strategic scenario experience approaches, ranging from exploration of new business approaches to the use in military planning.

Within the last year, we have performed several scenario experiences ranging from working to help high school students impacted by Katrina get involved in forensic investigations to our "Anticipating Terrorism" adventure that was simultaneously played out with national level experts and graduate students (the graduate students were about as good as the national level experts at coming up with realistic terrorist attacks).

Experiences like these generate the best value when they combine preparation, the right expertise, sound facilitation, detailed analysis, and results reporting. Preparation consists of understanding the problem space well enough to create a realistic scenario environment. Gathering the right expertise makes the experience work well and make sound progress. Facilitation takes people who know how to get group process to work well. Analysis requires specialized experts who research the key results and validate the results. The write-up requires skilled authors and structured presentation. The net effect is a valuable insight into alternatives, utilities and risks, and a meaningful review of the way forward.

## Mollie gets the last word in

Chile is chilly when California is warm. So here I am in a coat with gloves on when it's 90 degrees every day at home. That's the life of an international relater. Everything is not upside down here in the southern hemisphere, and opportunities abound in South America. Families are valued, my hosts are using me as a temporary replacement for their grown up daughter, and Internet access is good, even if phone access is expensive. But snow in July?!?