All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Three words you should never use in security and risk management

I thought about naming this article “The ill defined terms of security and risk management”, but I liked this one better. The three words?

> **Security:** For the most part, people that use this term don't seem to know how it is defined. It's kind of like the Supreme Court declaring with regard to pornography, “I know it when I see it”[1] Sadly, when Justice Stewart died, we were left with an ill-defined term of art again, and no official body to rule on a case by case basis to the same standard.
>
> **Risk Management:** This former word has been the subject of several articles at all.net over the years, including declaring it as a 4-letter word that ends in “k”. The latter word has a hope of proper use. But when combined, people who discuss risk management from the security perspective don't seem to know what that practice really is.

So naturally, I will violate my own declaration by using these words throughout this and other writings.

My qualifications in this regard

I plea guilty. For three years, I was the principal analyst for “Security and Risk Management Strategies” for Burton Group, a research and analysis firm. Leaving aside the term strategies for the moment, another thing most folks don't seem to know about, for that three year period, I personally worked and wrote on a daily basis about what we were calling security and risk management. During that time, and as far as I know since, we and they never properly defined these terms, nor did we or they particularly apply them in crisp and well-defined ways.

It's not that I didn't try. I did. But how many times can you really bring it up in a small group discussion before everyone knows that they don't know how to really defined the terms they are using? For those who want to know, it took only a few hours for the team I was working with to come to agree that we were talking about things we didn't fully understand, and over a period of years we came embrace our own use of the terms and the multiplicity of imperfect definitions associated with them.

Security

The term “security” in its various forms has been ill used for ages. No later than 1991, I wrote “Protection is something you do, not something you buy!”[2] From the 1980s, I used “information protection”, not “computer security”. Information being defined as symbolic representations in the most general sense, and protection being defined as keeping (people) from harm. I thought it was better than “the feeling of safety” (the definition of security according to the dictionary at that time) regarding computers.

[1] 378 USC 184, Jacobellis v. Ohio, 1964

[2] “A Short Course on Information Protection in Personal Computers and Local Area Networks”, (c) 1991, see http://all.net/books/pclansec.pdf.

Perhaps worse than the term “security” is the use of the term “secure” when describing almost anything. The notion that a computer is “secure” is, per the definition, ridiculous on its face. A person may feel secure about a computer doing something, but computers don't have feelings of safety because computers don't have feelings. I won't debate the issues of a sentient digital being for now, Mr. Data and other fiction not withstanding, and regardless of programs that emit sequences that may portend to feelings. It's not that those are invalid concepts, but rather, that they have not been applied to date to the issues as hand. A facility is not and can never be “secure” except relative to a particular set of event sequences and a set of defined outcomes. It is a relative term at best, and without the context, it is meaningless.

Risk Management

Management is something we may notionally understand. In essence, someone or some group is in charge of something and they are responsible and empowered to deal with it. They do so by their actions, taking feedback from their observations, and adapting (hopefully) to the situation as they observe it. But somehow, when it comes to risk management, most folks I encounter forget about the management part. They think it is some analytical process that has little human judgment or interaction involved. In my view. That's just completely off target. Risk management is presumably about managing risks, whatever they are, and it seems to me that all management is about managing risks to some extent. It's almost an oxymoron, but that's not quite the right term for it.

Risk is something I have written about a fair amount, and I will, for the moment, identify it, along with “reward”, as part of the same whole; a set of anticipated futures. We make decisions and act on them in order to achieve some desired future, realizing that what we desire may not come to pass, and that our acts may produce, in conjunction with the acts of others, a wide range of alternative outcomes, some of which we won't like. If we decide to call inaction another form of action (doing nothing is an act in itself), then everything we do assumes a risk and has the potential for a reward.

So risk management is decisions made by the people in charge of something with the knowledge of different outcomes as part of their decision-making process. Which is to say, it is management but assuming a lack of total ignorance. Which is to say, it is management. We could get rid of the term risk altogether and have more or less the same thing. Which is also to say that management is responsible for dealing with risks and rewards associated with their decisions. Any good manager tries to understand and take into account the potential outcomes of their decisions. Of course in the information space, most managers today don't know enough about the information-related risks to go it on their own. So they ask those who work in information technology to help them out. But of course the IT folks aren't usually all that savvy about risk-related issues either, so we get decisions that turn out badly. But even bad outcomes don't imply bad decisions. Risks and rewards go together. Bad outcomes don't mean the risk and reward were poorly balanced, although often they are, in my experience.

Summary

When you hear the words “security” and ”risk management”, beware. It is likely that they are being used by someone who doesn't understand what they are talking about, and thus misused. And by all means, avoid using them assuming that others understand what you are talking about. An old saying goes: “It is better to remain silent and be thought a fool than to open your mouth and remove all doubt”. In security and risk management, silence is golden.