Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The R word

In the security world, people commonly use a 4-letter word ending in 'k' as a foil to get what they want and stop what they don't want. But most of the people who use this word (we'll call it the "R" word, or simply [R]), can't tell you what it means when asked, or pop up with an answer that can't possible be right. They might say something like this:

[R] is the product of the consequences of an event times its likelihood.

They then often go and tell us to "assess [R]" by collecting a list of all of the possible events and calculating a probability for each, linking all events to consequences, and doing the simple arithmetic to calculate [R]. They may give an equation to make it look better:

$$R=\sum P(e)*C(e),\ \forall e\in E$$

I am willing to bet that they have never had to actually manage [R] and actually get usable answers.

The problems with [R] defined this way

There are few problems with this method of defining [R], to wit:

Given that $|E|=\aleph_0$, (the number of possible events is unlimited) and assuming that the time to perform any calculation is non-zero $(t>0)$, the time for calculating [R] for any given situation is infinite, $(t=\aleph_0)$ and thus cannot be done.

In addition, I note that there is also a lack of a historical or natural basis for calclating $P(e)$ for any $e\in E$. Indeed, at this time, there isn't a basis for identifying that $\exists e\in E$ as a random stochastic process, much less $\forall e\in E$ are such, or even that any $e\in E$ is of any particular mathematical structure. For this reason, the calculation method of multiplying a "probability" cannot be said to be appropriately applied in this context.

Then there is the problem of associating $C(e),\ \forall e\in E$. In addition to the now obvious fact that $|E|=\aleph_0$, and for $(t>0)$, $(t=\aleph_0)$ and thus $C(e)$ suffers from the same infinite time problems as $P(e)$, there is no method given for calculating $C(e)$ and thus it also has an undefined mathematical structure, and that means that we don't know how to calculate it. Historical evidence shows that, even after the realization of an event, the calculation of loss values from the event often varies by more than 4 orders of magnitude, and does not have a linear or well defined mathematical structure. Thus there is no method defined for performing a multiplication with it.

I should also note that given that $C(e)$ is in units of money and $P(e)$ is a pure number, and thus [R] is always a monetary value.

Note the especially careful way I have couched all of this in mathematical terms (and italicized in boldface) so as to make it harder to disagree with unless you are in the math "club".

So what is [R] really?

One of the best definitions I have seen of the R word goes something like this:

[R] is the potential that bad things could happen.

Note that, by the nature of the physics of the day, this is always a statement about the future, since physics does not admit to the potential for more than one past.

While we may seek to predict the future based on the past, such predictions are fraught with danger, as anyone who has prepared for a disaster of one magnitude and suffered a disaster of a greater magnitude will tell you, if they are still alive to do so.

You can take it or leave it

The thing about R is that you can't live without it. Everything ever done holds the potential that bad things could happen. But everything ever done also has the potential that good things could happen.

Reward is the potential that good things could happen.

[R] isn't just something to be avoided. In the classic management approach, [R] is also something to be taken in order to get rewards. It can be accepted (taken), avoided, transferred, or reduced (mitigated).

Making better decisions

The goal of managing [R] is to make good decisions. The first step to doing this is to understand the nature of the decisions being made. They are not, as a rule, ratio metrics that are quantitative in a continuous metric space. They tend to combine nominal, ordinal, interval, and ration metrics in a decision space wherein a choice from a limited number of qualitative alternatives must be made in different time frames depending on the situation. That means that they lend themselves largely to architectural decision-making for strategic issues.

The way to make better decisions in such a space is to have better knowledge, but the costs (part of [R]) of getting knowledge of the infinite set of "$P(e)*C(e), \forall e \in E$" is too high to bear. So the trick is to get enough information for better inform decision-making without paying more than that knowledge is worth. And there is another issue:

Knowledge of both [R] and rewards is required for sound decision-making.

Any decision based on [R] alone will be a bad one. If decision-makers ignore rewards, they end up doing nothing, the things they make decisions about decay naturally with time, and there is an eventual collapse. That is the nature of things (for the doubters among us, refer to the 2nd law of thermodynamics).

Conclusions:

The nature of the decision space is completely different than its typical depiction, and this is because, in attempting to define and refine it, the keys to its meaning have been lost.

Risk – the potential that bad things could happen – must be weighed against Rewards – the potential that good things could happen – and ...

Numbers alone are inadequate to express this tradeoff.

