Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Security metrics – a matter of type

When most people speak of metrics, they seem to be identifying continuously variable values over a smooth space with a "0" (i.e., "ratio" metrics). But in the information protection arena, we rarely have meaningful versions of such metrics, or anything like them. Rather, the metrics of protection today are of different types

What are the alternatives?

Generally, the metrics community identifies 4 different types of metrics; nominal, ordinal, interval, and ratio.

> **Nominal** metrics consists only of lists of things with no basis for formal comparison. Most human-oriented decision-support systems have some form of nominal metrics in the form of ideas, options, or other sets of possibilities that don't have any formal basis in an underlying scientific model.
>
> **Ordinal** metrics implies a partial ordering. Most decision support systems support some sort of comparison between like things or alternatives and this produces ordinal metrics.
>
> **Interval** metrics implies the ability to count things, but not against any standard. Many decision support systems provide for inputs in the form of counts of different sorts, used for things like voting.
>
> **Ratio** metrics implies the ability to add, subtract, compare, and normalize to a common zero value. Almost all decision support systems use ratio-based calculations, even if the underlying metrics are not ratio-based.

How do we use them?

Most decision-makers are familiar with these different ways of making decisions, and metrics of these types. To get a sense of this, it is important to recognize that, in the protection arena, we almost never have the option of a continuously tunable security mechanism that increases cost and effectiveness as we move some control. You either use a firewall or not. And if you do, you either allow a particular port or service or you don't, perhaps based on some other non-variable parameters, such as IP address or user identity. You don't have the option of having a 23.4% firewall with 96.4% coverage costing $1.93/day of operation and then tuning it up to a 32.8% firewall with 99.2% coverage for $2.92/day.

There are really only about 3 different quality levels of protective mechanisms, which I will call low, medium, and high surety. We generally advise enterprises to match the surety to the risk, which is to say, in this case, the worst case potential for negative consequences. If there are only 3 surety levels of protective mechanisms, what value can come to the decision maker from having more than 3 levels of risk? Spending more time, effort, and money on doing more precise measurements than the precision of the decision that has to be made is wasteful.

How do these metrics translate into decisions?

In our reference architecture for general decision-making, we identify the decision about the choice of metrics of this sort as follows:

> **IF** continuous functions that can be added, subtracted, multiplied, divided, and have a zero can be used to compare alternatives at a reasonable cost,
>
> > **THEN** use ratio metrics;
>
> **OTHERWISE IF** counting can be used to compare alternatives at reasonable cost,
>
> > **THEN** use interval metrics;
>
> **OTHERWISE IF** a partial ordering can be defined for comparing alternatives at a reasonable cost,
>
> > **THEN** use ordinal metrics;
>
> **OTHERWISE** only lists of alternatives exist with no common basis for comparison,
>
> > **THEN** use nominal metrics in the form of ideas, options, or other sets of possibilities that don't have any formal basis in an underlying scientific model.

Different types of metrics are used in different decision-making processes. Security decisions should be made based on the available and meaningful information.

For example, zoning strategy, which identifies the logical structuring of separation, cannot be made every day because of the costs and time involved in such structuring. There are only a few known alternatives that are supported by current technology and understanding. Roughly, they are;

- No zone separation,
- Several zones for different business functions,
- Many small zones for individual projects,
- Limited zoning with trusted mechanisms, or
- A small number of layered zones with subzones for risk disaggregation and functional separation.

With only 5 choices, ration metrics don't make sense. There isn't an obvious way to count things to make such a decision, but on the other hand, for larger numbers of things to be separated, economies of scale may come into play, and the notion of having thresholds to reduce process come into play as the number of zones becomes large. So an interval metric may be helpful in eliminating the “many small zones” option for large numbers of individual projects. The large number of possible contributing factors that are not directly comparable to each other (e.g., how services interoperate, expertise levels, costs, risk levels involved,, etc.) lead to the notion that a partial ordering may make sense when complex comparisons have to be made. Finally, there is an inherent nominal metric at play in that only 5 options are identified, thus limiting the choice to one of five alternatives without a “scientific” basis for making the decisions.

Making "better" security decisions

In the strict sense of "better" (i.e., the ability to compare alternatives against an optimization metric of some sort), it's hard to justify any particular decision-making process as the "best" for making the broad class of different decisions required in information protection today. And yet it seems clear that accepting the truth of the limitations of current knowledge demands that artificial methods that seek to put ratio metrics on all protection decisions be abandoned in favor of an alternative that fits more closely the reality of the decision-making processes actually used.

If we want to make better decisions we have to face and embrace this reality.

Once we abandon the notion of folding everything into ratio metrics, we are freed of the harness that such a discipline enforces and allowed to move into the realm of a broader range of decision-making approaches.

But with freedom comes responsibility

Just because we don't have real numbers that we can do arithmetic on doesn't mean that we are free to go wild. In fact, it's just the opposite. Because we don't have such numbers to lean on, we don't have the structure that the well studied mathematical fields bring us. We can't just make common assumptions, do statistics, arithmetic, run equations, and come up with a set of justified numbers that tells us what to do.

The responsibility of making better security decisions comes with the quality of the choices and the clarity of the explanations that justify the decisions by providing a rational basis for choosing between the alternatives. That deserves some more attention.

> **What are the reasonable alternatives?** In identifying alternatives, the most common mistake is to assume that you know what they are based on your experience. It is important to go through the history of the field and related fields to try to identify alternatives that are less obvious but may be more useful in special circumstances. This engages discussion surrounding what is missing from your analysis processes, and expands the notions of why the decision is important and how to make it.
>
> **How do we decide between them?** Deciding between alternatives means identifying the things that make them different from each other and how those differences relate to sound decision-making. This then feeds back into the reasonable alternatives, often eliminating what seem like alternatives and turning them into variations on a theme or adding alternatives to fill out the space identified in alternative identification.

Conclusions:

The nature of the decision space for information protection leads to different types of metrics for different situations (horses for courses), and in many cases, several different metrics types are involved. The desire to find a return on investment (ROI) or other single number to make security decisions is unlikely to work well, and it usually ends up costing more than it's worth.

Better decisions come from better understanding of the decision space.

Before putting numbers on protection decisions, it might be useful to get an understanding of the nature of the decisions and alternatives. Metrics aren't all numbers.

