A 4-Point Primer on FAIR to Share with Your Organization

1. We need to get the organization on not just the same page, but the right page with cyber risk…

The organization needs to get on the same page with the definition of cyber risk, a common vocabulary for discussing it, our goals for managing it, how it should be measured, and a way to compare and contrast solutions for managing it…

FAIR provides the clearest definition of risk: the probable frequency and magnitude of future losses the organization will face from adverse events, measured in financial terms.

FAIR provides a taxonomy (and lexicon) we can use to make sure we are all talking the same language

FAIR establishes the goal of cyber risk management clearly and in a way that is completely aligned to the business – it enables us to quantify risk in financial terms instead of using heat maps that tell us nothing about the losses we might face….all other forms of risk in the organization are evaluated in financial terms, cyber risk should be too.

The FAIR model – unlike qualitative approaches – allows us to conduct 'what if' analysis to evaluate the risk reduction impact of our cyber security investments

2. The goal of our cyber risk management program should be to limit future financial loss to within acceptable tolerances as cost effectively as possible…

Qualitative heat maps or maturity model approaches we are used to using show us nothing about the financial risk associated with cyber events – how much financial risk does a "red" risk represent? How much more risk is that than a "yellow?"

Without the quantified risk approach that FAIR enables, we're flying blind and making decisions that we cannot say for sure reduce risk at all.

3. We need an analysis method that expresses risk as frequency x magnitude…

An approach that focuses on trying to quantify risk using likelihood x impact doesn't allow us to actually quantify the potential losses we might face – it represents flawed attempts at math and it most definitely does not allow us to account for multiple potential loss events in a given timeframe.

Consider this small example scenario looking at how much risk we face over the next year from routine malware infections on employee laptops:

ANALYSIS MODEL	PROBABLE FUTURE LOSS
100% likelihood x $1,000 impact	**???**
118 malware infections (frequency) of laptops this year x $1,000 to remediate	**$118,000**

Despite it being so widely used as a reference for risk in cyber security, likelihood x impact is a flawed model that does not allow us to generate forecasts of risk in all cases. We need the real quantification method that FAIR enables and that allows us to look at potential ranges of outcomes in our analyses.

4. We need a methodology that accounts for uncertainty, allows for logical comparisons, drives out subjectivity and bias and that can be simply explained and defended…

There isn't a risk model that exists that is perfect – but FAIR helps us remove many of the flaws involved with current approaches.

Heat maps don't allow us to express our uncertainty about the impact of a cyber event – we're forced to choose a single rating when we know the realistic outcomes may range (across multiple of the pre-designated low/medium/high ratings/buckets) . FAIR solves this problem by showing us the potential range of impact in financial terms.

FAIR produces simple, logical risk analysis – qualitative methods are confusing and left open for subjectivity and interpretation.

FAIR provides a blueprint for analysis which is repeatable, explainable and defensible. It gives us the ability to compare risk reduction over time because we are sure the same steps are followed in every analysis we conduct.