Should I buy mobile phone insurance? A Quantitative Risk Analysis

It seems like I'm always losing or damaging my cell phone. I have two small children, so my damage statistics would be familiar to parents as well as shocking to those without kids. Over the last 5 years I've lost my cell phone, cracked the screen several times, had it dunked in water (don't ask me where), and several other mishaps. The costs definitely started to add up over time. So when it was time to re-up my contract with my mobile phone provider, Verizon, I decided to consider an upgraded type of insurance called **Total Mobile Protection.** The insurance covers such items as lost/stolen devices, cracked screens, and out-of-warranty problems.

The insurance is $13 a month or $156 a year, as well as a replacement deductible that ranges from $19 to $199, depending on the age of the device. The best way to determine if insurance is worth the cost, in this instance, is to perform a quantitative risk analysis. A qualitative analysis using adjectives like "red" or "super high" does not provide the right information to make a useful comparison between the level of risk versus the additional cost of insurance. If a high/medium/low scale isn't good enough to understand risk on a $600 iPhone, it shouldn't be good enough for your company to make important decisions.

To get started, I need two analyses: one that ascertains the current risk exposure without insurance, and another that forecasts potential risk exposure through partial risk treatment via transference (e.g. insurance). I'll use F.A.I.R. (Factor Analysis of Information Risk) to perform the risk analysis because it's extensible, flexible and easy to use.

The power and flexibility of the F.A.I.R. methodology and ontology really shines when you step outside cyber risk analyses. In my day job, I've performed all sorts analyses from regulatory risk to reputation risk caused by malicious insiders, and just about everything in between. However, I've also used F.A.I.R. to help make better decisions in my personal life when there was any degree of uncertainty. For example, I did an analysis a few years back on whether to sell my house, a 1879 Victorian home, or if I should sink money into a bevy of repairs and upgrades.

Insurance is also a favorite topic of mine: does my annualized risk exposure of a loss event justify the cost of an insurance policy? I've performed this type of analysis on extended auto insurance coverage, umbrella insurance, travel insurance and most recently, mobile phone insurance – the focus of this post. Quantitative risk analysis is a very useful tool to help decision makers understand the costs and the benefit of their decisions under uncertainty.

This particular risk analysis is comprised of the following steps:

- Articulate the decision we want to make
- Scope the analysis
- Gather data

- Perform analysis #1: Risk without insurance
- Perform analysis #2: Risk with insurance
- Comparison and decision

Step 1: What's the Decision?

The first step of any focused and informative risk analysis is identifying the *decision*. Framing the analysis, in the form of reducing uncertainty, when making a decision eliminates several problems: analysis paralysis, over-decomposition, confusing probability and possibility, and more.

Here's my question:

Should I buy Verizon's Total Protection insurance plan that covers the following: lost and stolen iPhones, accidental damage, water damage, and cracked screens?

Step 2: Scope the Analysis

Failing to scope out a risk assessment thoroughly creates problems later on, such as over-decomposition and including portions of the ontology that are not needed. Failing to properly scope a risk analysis upfront often leads to doing more work than is necessary.

Asset at Risk	iPhone 8, 64GB ($600, as of today's writing)
Threat Community	Me, children, thieves
Threat effect	Availability

Asset at risk: The asset I want to analyze is the physical mobile phone, which is an iPhone 8, 64GB presently.

Threat community: Several threat communities can be scoped. From my kids, to myself, to thieves that may steal my phone. Either taking it from me directly, or not returning my phone to me should I happen to leave it somewhere.

Go back to the decision we are trying to make and think about the insurance we are considering. The insurance policy doesn't care how or why the phone was damaged, or if it was lost or stolen. Therefore, scoping in different threat communities into the assessment is over-decomposition.

Threat effect: Good information security professionals would point out the treasure trove of data that's on a typical phone, and in many cases, is more valuable than the price of the phone itself. They are right.

However, Verizon's mobile phone insurance doesn't cover the loss of data. It only covers the physical phone. Scoping in data loss or tampering (confidentiality and integrity threat effects) is not relevant in this case and is *over-scoping* the analysis.

Step 3: Gather Data

Let's gather all the data we have. I have solid historical loss data, which fits to the Loss Event Frequency portion of the F.A.I.R. ontology. I know how much each incident cost me, which is in the Replacement cost category, as a Primary Loss.

Year	# of loss events	What it was	My Cost (no insurance)
2014	2	2 cracked screens	$90 each ($180 total)
2015	1	1 stolen phone	$600
2016	1	1 phone in the toilet	$600
2017	1	1 cracked screen	$90
2018 (YTD)	0		

Fig 1: Loss and cost data from past incidents

After gathering our data and fitting it to the ontology, we can make several assertions about the scoping portion of the analysis:

- We don't need to go further down the ontology to perform a meaningful analysis that aids the decision.
- The data we have is sufficient – we don't need to gather external data on the average occurrence of mobile device loss or damage. See the concept of the value of information for more on this.
- Secondary loss is not relevant in this analysis.

(I hope readers by now see the magic in forming an analysis around a decision – every step of the pre-analysis has removed items from the scope, which reduces work and improves accuracy.)

Fig 2: Areas of the F.A.I.R. ontology scoped into this assessment, shown in green

Keep in mind that you do not need to use all portions of the F.A.I.R. ontology; only go as far down as you absolutely need to, and no further.

Step 4: Perform analysis #1, Risk without insurance

The first analysis we are going to perform is the current risk exposure, without mobile phone insurance. Data has been collected (Fig. 1) and we know where in the F.A.I.R. ontology it fits (Fig. 2); Loss Event Frequency and the Replacement portion of Primary Loss. To perform this analysis, I'm going to use the free FAIR-U tool, available from RiskLens.

Loss Event Frequency
Refer back to Fig 1. It's probable that I could have a very good year, such 2018 with 0 loss events so far. On a bad year, I had 2 loss events. I don't believe I would exceed 2 loss events per year. I will use these inputs for the Min, Most Likely, and Max and set the Confidence at High (this adjusts the curve shape aka Kurtosis) because I have good, historical loss data that only needed a slight adjustment from a Subject Matter Expert (me).

Primary Loss
Forecasting Primary Loss is a little trickier. One could take the minimum loss from a year, $0, the maximum loss, $600, then average everything out for a Most Likely. However, this method does not accurately capture the full range of what could go wrong in any given year. To get a better forecast, we'll take the objective loss data, give it to a Subject Matter Expert (me) and ask for adjustments.

The minimum loss cost is always going to be $0. The maximum, worst-case scenario is going to be two lost or stolen devices in one year. I reason that it's entirely possible to have two loss events in one year, and it did happen in 2014. Loss events range from a cracked screen to a full device replacement. The worst-case scenario is $1,200 in replacement device costs in one year. The Most Likely scenario can be approached in a few different ways, but I'll choose to take approximately five years of cost data and find the mean, which is $294.

Let's take the data and plug it onto FAIR-U and run the analysis.

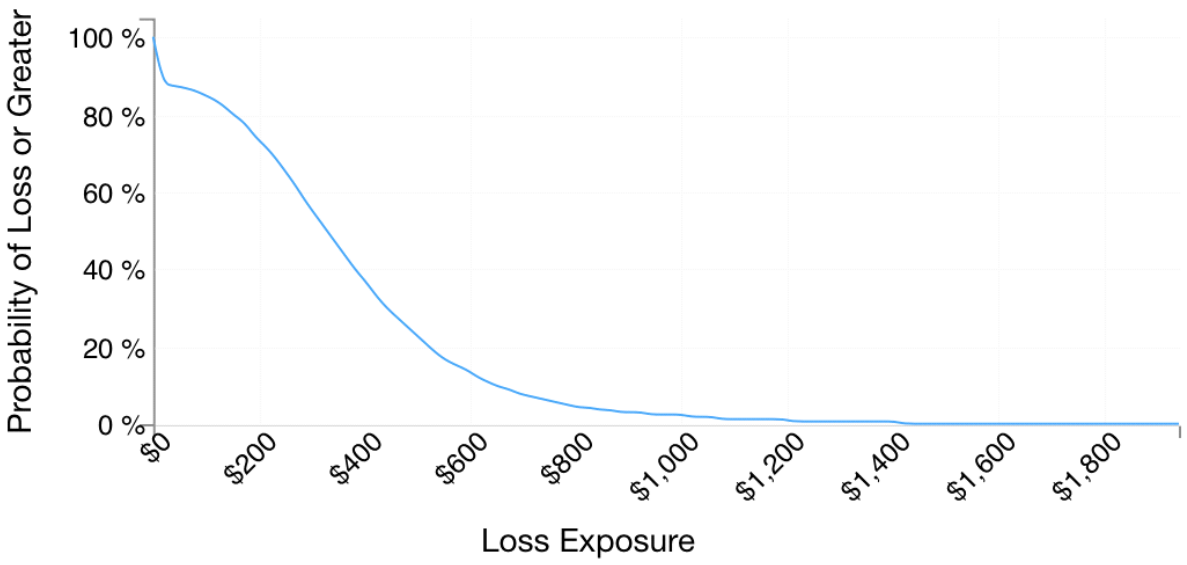
Risk Analysis Results

FAIR-U uses Monte Carlo to simulate thousands of years' worth of scenarios, based on the data we input and confidence levels, to provide the analysis below.

	Min	Avg	Max
Loss Events / Year	0	1	2
Loss Magnitude	$8	$353	$1.1k

Fig 3

Here's a Loss HYPERLINK "#"Exceedance Curve, which is one of many ways to visualize risk analysis results.



Step 5: Perform analysis #2: Risk with insurance

The cost of insurance is $156 a year plus the deductible, ranging from $19 to $199, depending on the type, age of the device, and the level of damage. Note that Verizon's $19 deductible is probably for an old-school flip-phone. The cheapest deductible is $29 for an iPhone 8 screen replacement. The worst-case scenario – two lost/stolen devices – is $554 ($156 for insurance plus $199 X 2 for deductible). Insurance plus the average cost of deductibles is $221 a year. Using the same data from the first analysis, I've constructed the table below which projects my costs with the same loss data, but with insurance. This lets me compare the two scenarios and decide the best course of action.

Year	# of loss events	What it was	My Cost (no insurance)
2014	2	2 cracked screens	$214 (insurance at $156, plus x2 deductibles at $29 each)
2015	1	1 stolen phone	$355 (insurance at $156, plus $199 deductible)
2016	1	1 phone in the toilet	$355 (insurance at $156, plus $199 deductible)
2017	1	1 cracked screen	$185 (insurance at $156, plus $29

			deductible)
2018 (YTD)	0		$0

Fig 4

Loss Event Frequency

I will use the same numbers as the previous analysis. Insurance, as a risk treatment or a mitigating control, influences the Loss Magnitude side of the equation but not Loss Event Frequency.

Primary Loss

To be consistent, I'll use the same methodology to forecast losses as the previous analysis.

The minimum loss cost is always going to be $0. The maximum, worst-case scenario is going to be two lost or stolen devices in one year, at $710 ($355 total per incident).

Most Likely cost is derived from the mean of five years of cost data, which is $221.

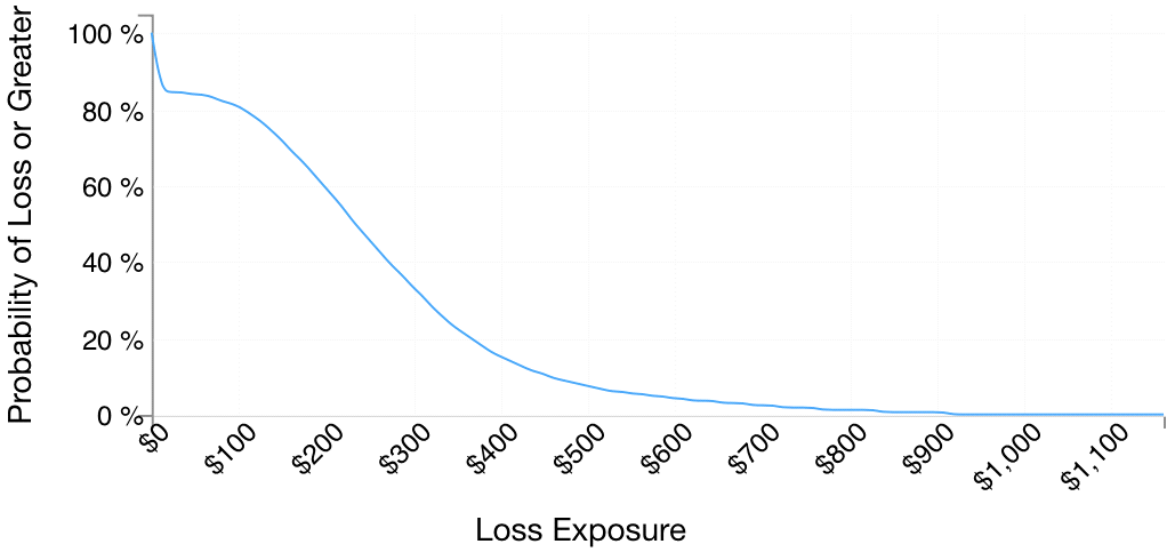
Risk Analysis Results

FAIR-U uses Monte Carlo to simulate thousands of years' worth of scenarios, based on the data we input and confidence levels, to provide the analysis below.

	Min	Avg	Max
Loss Events / Year	0	1	2
Loss Magnitude	$8	$247	$1.1k

Fig 5

The Loss Exceedance Curve:



Comparison

Without insurance, my average risk exposure is $353, and with insurance, it's $247. The analysis has provided me with useful information to make meaningful comparisons between risk treatment options.

Decision

I went ahead and purchased the insurance on my phone, knowing that I should rerun the analysis in a year. Insurance is *barely* a good deal for this year, and it was heavily influenced by the fact that I experience a total loss of phones at a higher rate than most people. I may also find that as my kids get older, I'll experience fewer loss events.

I hope readers are able to get some ideas for their own quantitative analysis. The number one takeaway from this should be that some sort of decision analysis needs to be considered during the scoping phase.

Further Analysis

There many ways that this analysis can be extended too, such as:

- Does the cost of upgrading to an iPhone XS reduce the loss event frequency? (The iPhone XS is more water resistant than the iPhone 8)
- Can we forecast a reduction in Threat Capability as the kids get older?
- Can we find the optimal set of controls that provide the best reduction in loss frequency? For example, screen protectors and cases of varying thickness and water resistance. (Note that I don't actually *like* screen protectors or cases, so I would also want to measure the utility of such controls and weigh it with a reduction in loss exposure.)

Any questions or feedback? Let's continue the conversation in the comments below.