![RiskLens™]

BALD TIRE

Understanding the need to move information risk management from art toward science

Jack Jones, CISSP, CISM, CISA

Bald Tire Scenario

As you proceed through each of the steps within the scenario below, ask yourself how much risk is associated with what's being described.

- Picture in your mind a bald car tire. Imagine that it's so bald you can hardly tell that it ever had tread. How much risk is there?

- Next, imagine that the bald tire is tied to a rope hanging from a tree branch. How much risk is there?

- Next, imagine that the rope is frayed about halfway through, just below where it's tied to the tree branch. How much risk is there?

- Finally, imagine that the tire swing is suspended over an 80-foot cliff – with sharp rocks below. How much risk is there?

Now, identify the following components within the scenario. What were the:

- Threats
- Vulnerabilities
- Risks

Scenario Analysis

Most people believe the risk is 'High' at the last stage of the Bald Tire scenario. The answer, however, is that there is very little probability of significant loss given the scenario exactly as de-scribed. Who cares if an empty, old bald tire falls to the rocks below?

Was my question about the amount of risk unfair? Perhaps, and I've heard the protests before…"But what if someone climbs on the swing?" and, "The tire's purpose is to be swung on, so of course we assumed that somebody would eventually climb on it!" Both are reasonable arguments. My point is that it's easy to make assumptions in risk analysis. In fact, some assumptions are unavoidable because it's impossible to know every conceivable factor within a risk scenario. However, assumptions about key aspects of the risk environment can seriously weaken the over-all analysis.

The second point I'd like to make is that, from any group that goes through the Bald Tire scenario, I'll typically get several different descriptions of what constitutes the threat, vulnerability, and risk within the scenario. I've heard the frayed rope described as threat, vulnerability, and risk. I've also heard the cliff and rocks described as threat, vulnerability, and risk. The simple fact is that we, as a profession, have not adopted standard definitions for our terms. In informal discussions amongst ourselves, this may not always be a significant problem, as we typically understand what is meant by the context of the conversation. Consider, however, that physicists don't confuse terms like mass, weight, and velocity, and financial professionals don't confuse debit and credit – even in informal discussions – because to do so significantly increases the opportunity for confusion and misunderstanding.

This is important to keep in mind when we're trying to communicate to those outside our profession – particularly to sharp executives who are very familiar with the fundamental concepts of risk – where misuse of terms and concepts can damage our credibility as professionals and reduce the effectiveness of our message.

A third point is that **you can't have significant risk without the potential for significant loss**. In other words, it doesn't matter how exposed to harm an asset is, if the asset ain't worth much, the risk ain't high. This is because risk **always** includes a value component. If it didn't, betting a million dollars would be equivalent to betting one dollar.

A final point is that there's a tendency to equate vulnerability with risk. We see a frayed rope (or a server that isn't properly configured) and automatically conclude that the risk is high. Is there a correlation between vulnerability and risk? Yes. Is the correlation linear? No, because vulnerability is only one component of risk. Threat event frequency and loss magnitude also are key parts of the risk equation.

So, what are the asset, threat, vulnerability, and risk components within the Bald Tire scenario? The definitions and rationale are described more specifically further on, but, simply stated:

- The asset is the bald tire
- The threat is the earth and the force of gravity that it applies to the tire and rope
- The **potential** vulnerability is the frayed rope (disregarding the potential for a rotten tree branch, etc.)

What about risk? Which part of the scenario represents risk? Well, the fact is, there isn't a single component within the scenario that we can point to and say, "Here is the risk." Risk is not a thing. We can't see it, touch it, or measure it directly. Similar to speed, which is derived from distance divided by time, risk is a derived value. It's derived from the combination of threat event frequency, vulnerability, and asset value and liability characteristics.

Having made an issue of terminology, the following paragraphs introduce and briefly discuss some basic definitions.

Threat

A reasonable definition for Threat is anything (e.g., object, substance, human, etc.) that is capable of acting against an asset in a manner that can result in harm. A tornado is a threat, as is a flood, as is a hacker. The key consideration is that threats apply the force (water, wind, exploit code, etc.) against an asset that can cause a loss event to occur.

Vulnerability

You may have wondered why "potential" is emphasized when I identified the frayed rope as a potential vulnerability. The reason it's only a potential vulnerability is that we first have to ask the question, "Vulnerable to what?" If our frayed rope still had a tensile strength of 2000 pounds per square inch, its vulnerability to the weight of a tire would, for all practical purposes, be virtually zero. If our scenario had included a squirrel gnawing on the frayed rope, then he also would be considered a threat, and the rope's hardness would determine its vulnerability to that threat. A steel cable – even a frayed one – would not be particularly vulnerable to our furry friend. The point is that vulnerability is **always** dependent upon the type and level of force being applied.

Asset

In the context of information risk, we can define Asset as any data, device, or other component of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss. The question is often asked whether corporate reputation is an asset. Clearly, reputation is an important asset to an organization, yet it doesn't qualify as an information asset given our definition. Yes, reputation can be damaged, but that is a downstream outcome of an event rather than the primary asset within an event. For example, reputation damage can result from public disclosure of sensitive customer information, but the primary asset in such an event is the customer information.

Risk

The following definition applies regardless of whether you're talking about investment risk, market risk, credit risk, information risk, or any of the other commonly referenced risk domains:

Risk – The probable frequency and probable magnitude of future loss

In other words – how often something bad is likely to happen, and how much loss is likely to result. As stated above, these probabilities are derived from the combination of threat, vulnerability, and asset characteristics.

Other Factors

So, where do the cliff and rocks fit into the risk equation? They aren't threat agents because they don't precipitate an event and, clearly, they aren't vulnerabilities that allow an event to occur. Consequently, these components can be considered secondary loss factors because their existence contributes to the magnitude of loss from an event. A real world example would be the fines and sanctions levied by regulatory agencies following an information security event. The regulations and regulators aren't the agents that commit a breach, so they aren't threats in the context of the event. They also aren't a technological, procedural, or other weakness that allowed the breach to occur. Nonetheless, they play a role in how much loss occurs and therefore must be included in our risk analysis. (Note, however, that there are scenarios in which regulators can be classified as threat agents – i.e., when they perform an audit.)

The Bald Tire Metaphor

Information risk management today is practiced as an art rather than a science. What's the difference? Science begins by analyzing the nature of the subject – forming a definition and determining the scope of the problem. Once this is accomplished, you can begin to form and then substantiate theories and hypotheses, which provide deeper understanding. This deeper understanding provides the means to explain and more effectively manage the subject.

Art, on the other hand, doesn't operate within a clearly defined framework or definition. Consequently, it's not possible to consistently explain or calculate based upon an artistic approach. A useful example is shamanism. The shaman rolls his bones or "confers with the gods." He then prescribes a remedy based upon what his forefathers have passed down to him ("best practices"). Now, some shamans may be extremely intuitive and sensitive to the conditions within a scenario and may be able to select a reasonable solution on most occasions. But the shaman can't rationally explain his analysis, nor can he credibly explain why the cure works (or sometimes doesn't work). And, while we would like to believe that best practices are generally effective (as we tend to reuse what we believe has been successful in the past), this may be a dangerous assumption.

Best practices are often based on long-held shamanistic solutions, tend to be one-size-fits-all, may evolve more slowly than the conditions in which they're used, and can too often be used as a crutch – e.g., "I can't explain why, so I'll just point to the fact that everyone else is doing it this way."

There is, however, no question that intuition and experience are essential components of how we do our jobs. The same is true for any profession. Yet these alone don't provide much traction in the face of critical examination, and are not strong formulas for consistency.

Putting Tread on the Tire

Recently, our profession has begun to pay a significant amount of attention to metrics. A word of caution – metrics and science are not the same thing. I can measure some parameter or count the instances of some event, but if I haven't developed a logical and rational understanding of the broader context within which the metric applies, all I have is numbers. Furthermore, in the absence of a fundamental understanding of the subject, it's far too easy to misinterpret and misuse the data. Bottom line -- in order for metrics to be truly useful, we have to understand our subject well enough to know how the metrics affect our objective. Specifically, how they affect the frequency and magnitude of loss.

We can't consistently and effectively manage what we can't measure – and we can't measure what we haven't defined. The first thing we need to do to shift from art to science is define our subject. What exactly is information risk? What are the factors that make it up, and how do they relate to one another? After we've defined our subject, how do we measure it? How do we model and evaluate the complex risk scenarios we face? Finally, if we've managed to accomplish all of these things, how do we articulate risk to the decision- makers who need this information?

Factor Analysis of Information Risk (FAIR) provides a reasoned and logical framework for answering these questions:

- **A taxonomy** of the factors that make up information risk. This taxonomy provides a foundational understanding of information risk, without which we couldn't reasonably do the rest. It also provides a set of standard definitions for our terms.

- **A method for measuring** the factors that drive information risk, including threat event frequency, vulnerability, and loss.

- **A computational engine** that derives risk by mathematically simulating the relationships between the measured factors.

- **A simulation model** that allows us to apply the taxonomy, measurement method, and computational engine to build and analyze risk scenarios of virtually any size or complexity.

About the author

Jack is the foremost authority in the field of information risk management. As the President of the FAIR Institute and the co-founder and EVP R&D at RiskLens™, he continues to lead the way in developing effective and pragmatic ways to manage and quantify information risk. As a three times Chief Information Security Officer (CISO) with forward-thinking financial institutions such as Nationwide Insurance, Huntington Bank and CBC Innovis, he received numerous recognitions for his work, including: the ISSA Excellence in the Field of Security Practices award in 2006; a finalist award for the Information Security Executive of the Year, Central US in 2007; and the CSO Compass Award in 2012, for advancing risk management within the profession.

Prior to that, his career included assignments in the military, government intelligence, consulting, as well as the financial and insurance industries. Jack is the author of FAIR, the only international standard VaR model for cyber security and enterprise technology. A sought-after thought leader, he recently published 'Measuring and Managing Information Risk: A FAIR Approach' and is a regular speaker at industry conferences.

RiskLens™

850 E Spokane Falls Blvd, Ste 270
Spokane, WA, USA 99202

11911 Freedom Drive, Ste 850
Reston, VA, USA 20190

Toll Free: 866.936.0191
Web: www.RiskLens.com

About RiskLens™

RiskLens™ is the premier provider of cyber risk management software. RiskLens™ empowers large enterprises and government organizations to manage cyber risk from the business perspective by quantifying it in dollars and cents. Our customers leverage RiskLens™ to understand their cyber risk exposure in financial terms, prioritize their risk mitigations, measure the ROI of their security investments, and optimize their cyber insurance coverage.

RiskLens™ is the only cyber risk management software purpose-built on FAIR, the only international standard Value at Risk (VaR) model for cyber security and operational risk.