RiskLens

An Executive's Guide to Cyber Risk Economics

DECISION-MAKERS DESERVE A BETTER PICTURE OF CYBER RISK

BY JACK JONES
CHAIRMAN, FAIR INSTITUTE
EXECUTIVE VICE PRESIDENT R&D, RISKLENS

WWW.RISKLENS.COM
THE LEADER IN CYBER RISK QUANTIFICATION

Table of Contents

INTRODUCTION

Decision-makers Deserve a Better Picture of Cyber Risk

Cybersecurity risk has emerged as a top-three worry for large corporations as cyber attacks, online fraud and internal threats make a material impact on the business.

And, while boards and executives expect to be informed about cyber risk, very few of them seem to be getting the answers they want. Too often, cyber risk reporting is filled with technical jargon and colorful but hard to understand charts. Those responsible for cybersecurity—from the CEO on down—are urgently looking for better ways to measure risk and enable well-informed decision-making, regarding questions like:

- What are their organization's top cyber risks and how much exposure do they represent?
- Which cyber risk management investments matter most?
- Are they investing enough (or too much) in cyber risk management?

This e-book is intended to provide a straightforward, high-level guide for executives on economically-driven cyber risk management—i.e., prioritizing effectively, making trade-offs and choosing cost-effective solutions. It isn't a "how-to" manual, but instead, will help you recognize the challenges associated with common risk management methods, understand your options and choose a best-fit approach. Along the way it will discuss common concerns regarding quantitative cyber risk measurement and describe a pragmatic approach to cyber risk quantification.

By the way, although we use the term "cyber risk" in this document, the problems and solutions discussed here apply equally to information assurance, technology risk and even operational risk.

CHAPTER 1

You Can Be Compliant and Still Be in the Dark

What's Wrong with the Checklist Approach to Cyber Risk Management?

On the surface, it makes perfect sense—the more boxes your organization can check on an industry-standard "compliance" list, the more "mature" it is. And the more closely aligned it is with the herd (your peers in the industry), the better off you should be from a risk perspective. This reliance on relative measurements is a form of "implicit risk management," i.e., more boxes/maturity/alignment implies less risk. The problem is that none of those measurements provide real insight into how much risk exists or how risk levels will change if this, that, or the other event takes place.

Although compliance checklists are useful and sometimes even necessary, these "more is better" measurements fundamentally do not support prioritization or cost-benefit analyses. You end up asking yourself: which of the unchecked boxes or maturity deficiencies should we work on first? For that matter, how much risk reduction do we get for checking one box versus another, or climbing one more rung in the maturity scale? Compliance checklists, maturity models and benchmarks will never answer those questions. To fill the void, what commonly happens is that someone will wave a wet finger in the air and try to answer those questions based on what their gut tells them.

The alternative is what we refer to as "explicit" risk measurement, which involves measuring risk in terms of event likelihood and impact to the organization. This can be done qualitatively (for instance, on a "high-medium-low" scale) or quantitatively (using a computational model that generates probabilistic and economically-focused results), but there are significant limitations to qualitative risk measurements.

We'll get into these limitations in a later chapter. For now, simply recognize that explicit risk measurement enables both effective prioritization of risks and optimization of risk management solutions—**if measurement is done well.**

CHAPTER 2

The Current State of Cyber Risk Measurement

Fuzzy Thinking, Bogus Math, Missing Skill Sets...

Unfortunately, common cyber risk measurement practices today don't reliably provide executives with the information they need to make well-informed decisions. The result is an inability to recognize and deal with the organization's most critical exposures, and wasted resources spent on expensive risk management solutions.

There are a number of common factors inhibiting reliable cyber risk measurement today, including:

- Imprecise terminology
- Undefined scope
- Inaccurate models
- Bogus math
- Missing skill sets

The good news is that these don't have to be difficult or expensive to correct.

In our experience working with organizations of various sizes in various industries, we've found that between 70% and 90% of the "high risk" issues these organizations are focused on do not, in fact, represent high risk. As a result, resources are being allocated to concerns that shouldn't be a priority. Besides being wasteful, this means that truly significant problems are often being placed on the back burner simply due to resource constraints.

Imprecise Terminology

How enthusiastic would you be to ride a space shuttle mission if you knew that the engineers and scientists who planned the mission and designed the spacecraft couldn't agree on the definition of mass, weight and velocity? We have yet to meet a willing passenger for that voyage, yet that is exactly the state of terminology within the cyber risk field. Foundational terms like "risk" and "threat" are used with glaring inconsistency. This not only profoundly affects the ability to measure risk reliably, but it also impedes the ability to communicate effectively amongst peers and with decision-makers.

This is such a pervasive and fundamentally important problem that we provide an entire white paper on the topic here. (http://bit.ly/2q0qdzD)

Undefined Scope

It's common to see gaps identified through NIST CSF (or other such frameworks) described as "high risk" in the cyber realm.

- But what assumptions underlie that measurement?
- What are the assets at risk?
- Who or what are the threats to those assets?
- What compensating controls might be in place?

The point is that very often the things being rated as high/medium/low risk are rated without a clear understanding of key assumptions or scope. For example, the relevance of a deficient control condition can only be determined within the context of risk scenarios where that control is relevant.

Without that clarity, there are two significant problems:

1. There is a much higher probability of inaccurate measurement
2. The underlying assumptions can't be challenged by decision-makers

The bottom line is that you can't reliably measure (qualitatively or quantitatively) something that is ambiguously defined, and most risk measurements today are not founded on a clear understanding or articulation of the things being measured.

Inaccurate Models

The most common model being used to measure cyber risk today is the mental model of the individual risk analyst. In other words, cyber risk measurement quality is largely dependent upon how well practitioners understand the complex array of risk factors that are in play when proclaiming something to be high/medium/low risk. When combined with the terminology and scope challenges mentioned above (and the inherently complex nature of the problem space) the odds of accurate measurements diminishes significantly.

Beyond the challenges with mental models is the fact that several of the formal models commonly used today are fundamentally flawed.

Read a blog post (http://bit.ly/2rvjAXd) describing a serious flaw in the NIST 800-30 model.

Bogus Math

Performing mathematical operations on ordinal (i.e. such as 1-5 or red-yellow-green) scales generates unreliable and often misleading results. For example, few people would feel comfortable multiplying "red" times "yellow," or "high" times "medium." However, it is common to see those colors or words replaced with ordinal numbers, and then math—sometimes even quite complex math—is used to generate risk measurements. In his book, "The Failure of Risk Management," Douglas Hubbard refers to this as "worse than useless" because his research has shown that it consistently misinforms. Unfortunately, the practice of using math on ordinal numeric scales for risk measurement is widespread. Some risk management products have even baked this into their technologies, and most home-grown spreadsheet solutions do this, which almost invariably generate unreliable results.

Missing Skill Sets

The truth of the matter is that very few cyber security, audit, or risk professionals are trained in risk measurement principles and methods. To be sure, they may be brilliant at one or more aspects of the cyber risk landscape—controls assessments, policy development, threat intelligence, auditing, forensics, secure application development, etc.—but that does not qualify someone to measure risk.

Risk measurement (whether qualitative or quantitative) is an analytic process that involves explicitly scoping risk scenarios and then gathering information regarding threats; asset value and liability characteristics, and control conditions relevant to those scenarios. This information is then applied to a model in order to generate a clearer and more accurate understanding of risk.

Unfortunately, most of the risk measurement taking place in organizations today is not being performed by people who apply any rigor. The "wet finger in the air" predominates. To be clear, this is not a matter of poor professionalism or intentional neglect, but instead a reflection of how immature the industry is right now.

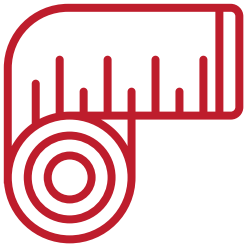
The skills required for reliable risk analysis include:

- ✓ Strong critical thinking skills
- ✓ An understanding of basic probability principles
- ✓ Training in calibrated estimation
- ✓ Being comfortable with numbers (no PhD required)
- ✓ Familiarity with decision support technologies (e.g., Monte Carlo functions)

As long as risk is being measured or "rated" by personnel who don't have specific analysis skills, training, and experience, the quality of risk management will continue to be problematic.

CHAPTER 3

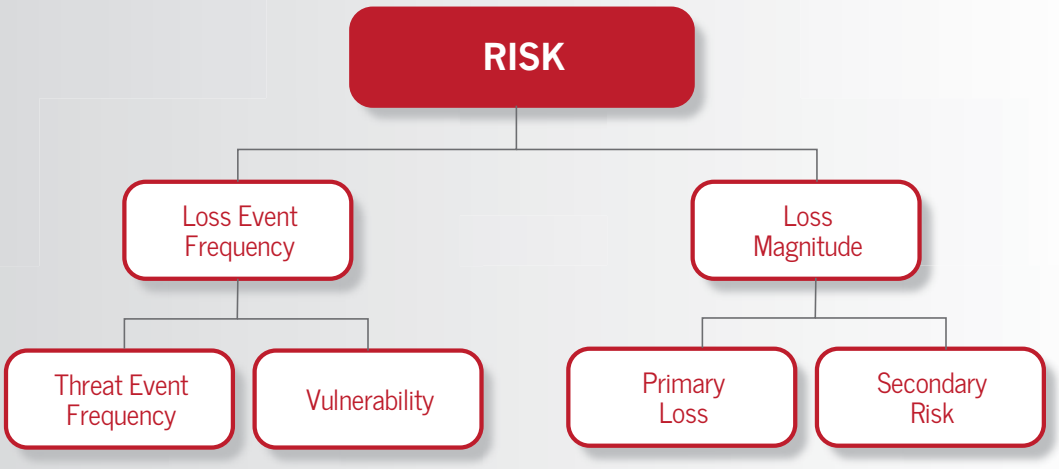
Introducing FAIR: How Risk Gets Quantified



A Disciplined Model for Measuring Risk Yields Actionable Results

Fortunately, it doesn't require rocket science to solve the problems outlined above. **Factor Analysis of Information Risk (FAIR)** is an open international standard risk model developed specifically to enable effective risk measurement and answer executive-level questions regarding cyber, technology and operational risk.

FAIR has been described as an intuitive codification of risk that clarifies and simplifies risk measurement and communication. At the core, it is a model (partially shown in the figure below) that describes the required elements for measuring risk.



Detailed descriptions of the model can be found in the Resources section at the end of this e-book. For now, simply recognize that the model serves as the foundation for accurate and reliable risk measurement and clear communication of those measurements.

The benefits FAIR brings to the table, include:

- ✓ Clear definitions for each of the risk factors, which normalize terminology and reduces confusion
- ✓ Serves to normalize the mental models of personnel tasked with measuring risk, which helps to ensure clear risk analysis scoping and measurement
- ✓ Acts as a framework for critically thinking through an analysis, which reduces the chance that important factors will be overlooked or double-counted, and helps to surface key assumptions being made in an analysis
- ✓ Describes the relationships between elements, which enables robust quantitative analysis using well-established methods like Monte Carlo simulations
- ✓ Is flexible, and can be applied in a triage-like manner or in great depth, as need and resources dictate

The bottom line is that personnel trained in FAIR can perform much higher quality risk analyses than are typical in the industry today.

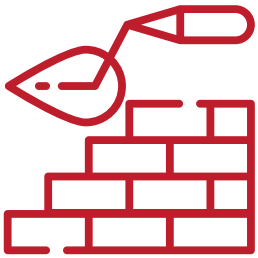
Resources for personnel who want to learn more can be found at:

1. The FAIR Institute, which is an expert, non-profit organization dedicated to developing standard risk management based on the FAIR methodology: www.fairinstitute.org
2. The Open Group, which has established FAIR as an international standard and provides educational resources and a professional certification in FAIR: www.opengroup.org/security
3. RiskLens, which provides FAIR training for individuals or entire teams within organizations: www.risklens.com

A number of universities have also begun to include FAIR in their curricula, and it is referenced by the US Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), as well as in proposed updates to cyber security standards by US federal banking regulators.

CHAPTER 4

Advantages of a Quantitative Approach to Cyber Risk



A Solid Foundation For Prioritization and Cost-Benefit Analysis

Every organization is subject to resource constraints, which means managing risk cost-effectively is necessary in order to appropriately balance risk management with other business imperatives. However, because of the tendency to rely on relative risk measurements (in addition to the problems described in Chapter 2), most organizations don't achieve this balance.

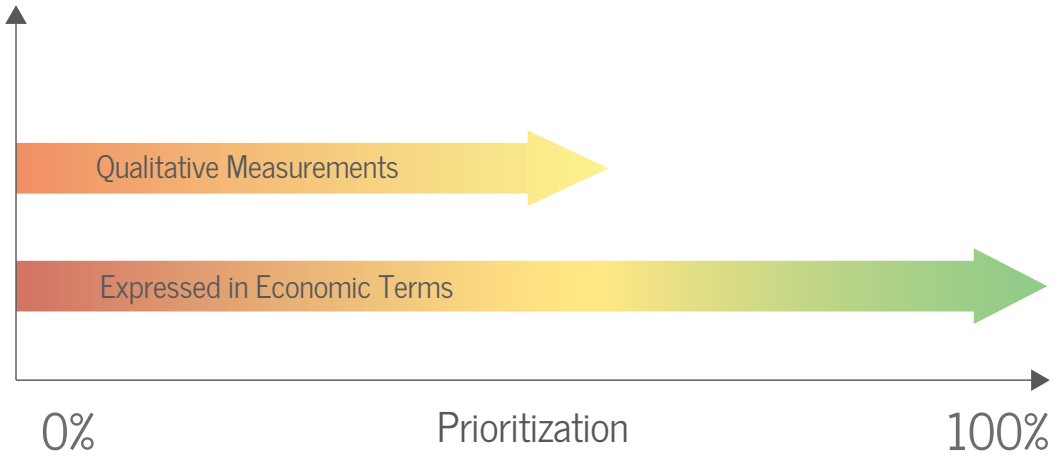
There are two dimensions that determine cost-efficacy in risk management:

1. The ability to identify and focus on your most important risks (i.e., prioritization)
2. The ability to understand the value proposition of risk mitigation projects and optimize your solution choices through cost-benefit analysis

Organizations that are effective in both of these dimensions reduce the odds of painful surprises and wasted resources. With this in mind, it's important to recognize the degree to which qualitative and quantitative measurements support these dimensions.

Prioritization

Organizations can make significant improvements in their ability to prioritize among risks simply by avoiding or correcting the problems described in Chapter 2, even if still measuring risk qualitatively. This will only take them so far, however, because qualitative measurements are inherently so imprecise. For example, an organization might become very good at accurately putting risks into the right high/medium/low buckets, but they will not be able to differentiate risks within these buckets—i.e., they won't know which "high risk" is highest. Accurately differentiating within buckets requires quantitative measurements. The diagram below provides a comparison between how far qualitative measurements can support prioritization, versus quantitative measurements.

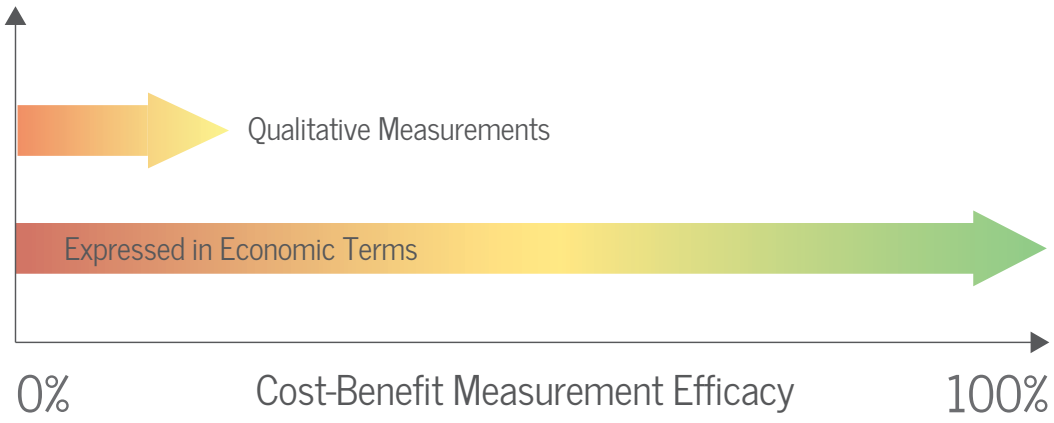


SOURCE: RISKLENS.COM

Choosing Cost-Effective Solutions

Once you're able to focus on your most important risks, the next step is being able to choose your most cost-effective solutions. This is where qualitative measures fall flat for two reasons. First, in many cases they are simply too imprecise to effectively reflect differences in the level of risk reduction from various solutions. Second, they don't reflect risk reduction in meaningful business terms. Going from "high" to "medium" might sound and even feel good, but what does it actually mean? The diagram below provides a comparison between how far qualitative measurements can support cost-benefit analysis, versus quantitative measurements.

The bottom line is that improving your organization's ability to measure risk qualitatively is a start toward managing risk cost-effectively. To become good at cost-effective risk management though, you need to leverage quantitative measurements. This enables you to understand how much less risk is likely to exist after a control is improved. It also allows you to understand how much more risk is likely to exist if a control is removed or loosened for business efficiency or cost-saving reasons.



SOURCE: RISKLENS.COM

Another key limitation of qualitative risk measurements is that you can't aggregate them in a meaningful and accurate manner, nor can you understand how much risk a single concern adds to the overall risk profile.

CHAPTER 5

How to Get Started with Quantification

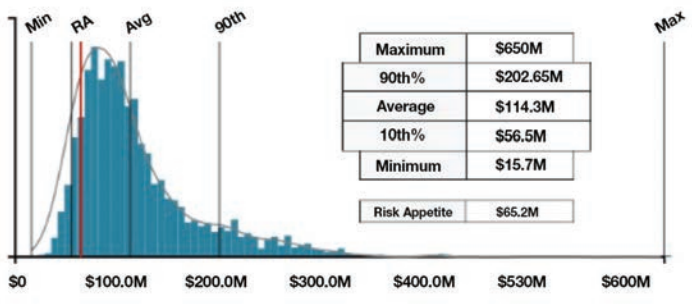
Answers to 3 Common Questions

1. What Do the Numbers Tell Me?

There are various risk measurement solutions that express risk numerically, but not all numeric values have the same level of meaningfulness. For example, what does it mean if your organization was given a risk "score" of 756? By itself that number is meaningless. If, however, you were told that it's a credit rating-like score and that 756 puts your organization in the top 25th percentile of your industry, then suddenly you have a relative understanding of where the organization stands within the herd. This may be useful and comforting, but it certainly isn't going to help you prioritize your risks in business terms or choose cost-effective solutions.

The point is that many in the risk industry will say they're quantifying risk when using these numeric, but still relative, values. More often than not, however, those numbers represent control conditions, which is just one element in a risk measurement. **In order to achieve cost-effectiveness, risk has to be measured in probabilistic and economic terms.** The illustration below provides an example of an analysis based on the FAIR standard.

HOW MUCH RISK DO WE HAVE?



SOURCE: RISKLENS.COM

These values represent the annualized loss exposure associated with one or more risks (loss event scenarios). As you can see, it provides a clear representation of the range of loss exposure—from the "most likely" to the "extreme" ends of the spectrum. In the next chapter we'll provide examples of how expressing risk in this form leads to better prioritization and solution selection.

2. How Much Data Do I Need?

Despite rapidly growing adoption of FAIR, there are those in the industry who voice concerns regarding quantitative cyber risk analysis. Very often, the basis for their concerns revolve around data quantity and/or quality. In other words, if we have sparse data in a dynamic landscape, how confident can we be in a quantitative analysis? It's an important question.

The truth is, whether you're measuring risk with your gut or a supercomputer, the data are what they are. In other words, someone's measurements don't improve simply because they don't apply analytic rigor and use high/medium/low as their risk measurements. **At least with quantitative analyses there are well-established methods (e.g., PERT distributions, Monte Carlo simulations and calibrated estimation techniques) for dealing with sparse and uncertain data and reducing the effects of human subjectivity.**

If anything, this enables quantitative measurements to be more reliable than qualitative ratings. These methods also enable you to reflect uncertainty through results shown as distributions, which is not possible when risk is simply rated as high/medium/low.

3. How Much Effort Will It Take?

The age-old adage "You get what you pay for" applies to risk management, too. If your organization invests virtually no analytic rigor when measuring risk, and personnel simply proclaim things to be "high/medium/low risk" based on their intuition, then nobody should be surprised when the results are unreliable. On the other hand, our experience has shown that the law of diminishing returns also applies to analytic rigor. This is good news because it means that a modest increase in analytic effort can drive significant improvements in quality, particularly when leveraging a strong risk analysis technology.

The bottom line is that an organization can effectively manage the level of effort it applies to risk analysis. This is accomplished through a triage process that identifies which risks or risk-related questions benefit most from more in-depth analyses, versus analyses that are more quick-and-dirty in nature. It is important, however, for even simpler analyses to be based on the same analytic model to help ensure consistency.

Risk analysis software applications can also dramatically reduce the level of effort. With that in mind, there is strong temptation for software solution providers to keep user inputs and outputs as simple as possible. Although that intuition is directionally correct, it can and often has been taken too far. There's a reason Einstein said (in effect), "Make things as simple as possible, but not simpler." Oversimplification of risk measurement and reporting leads to inaccuracy, misinterpretation and poor risk management decisions.

Red Flags

There are a few red flags you should keep in mind when evaluating quantitative risk measurement solutions.

- *It's never a good sign when a quantitative solution expresses risk as a single discrete value (e.g., $500,000). That isn't how risk works. There is simply too much uncertainty and variability in the landscape for that kind of precision. Measurements and results need to faithfully reflect that uncertainty and be presented as ranges or distributions of probabilities.*

- *It also should be concerning when you get a probabilistic and economic description of risk without having to enter any quantitative values related to likelihood or impact. You can't just plug something into the network or check some boxes and have the solution spit out a loss exposure result without questioning those results.*

- *The big questions in your mind should be: "What's going on under the covers?" "What are the assumptions being made?" and "Where are the numbers coming from?"*

- *If the loss exposure doesn't include a timeframe component (e.g., annualized) then there is no context for understanding the likelihood of the event materializing.*

CHAPTER 6

FAIR and Risk Quantification in Action

Examples of Risk Prioritization, Cost-Benefit Analysis and More

In order to be pragmatic, a solution has to achieve its intended benefit with minimal effort—in this case, striking the right balance between effort and information quality. In this chapter, we'll provide examples of how this can be accomplished. Note that these examples were generated using the RiskLens (www.risklens.com) cyber risk quantification solution that was purpose-built on FAIR.

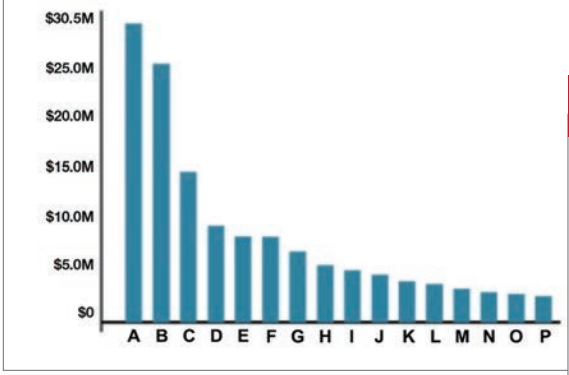
Prioritization and Cost-Benefit Analysis

Prioritization use-cases run the gamut from tactical to strategic. Examples include, but aren't limited to:

- Identifying the organization's Top 10 cyber and technology risks
- Understanding which of several audit findings represent the most risk
- Identifying which business units or business processes are contributing the most risk to the organization
- Recognizing which of the organization's technologies introduce the most risk
- Understanding which remediation and/or response activities will provide the greatest bang-for-the-buck

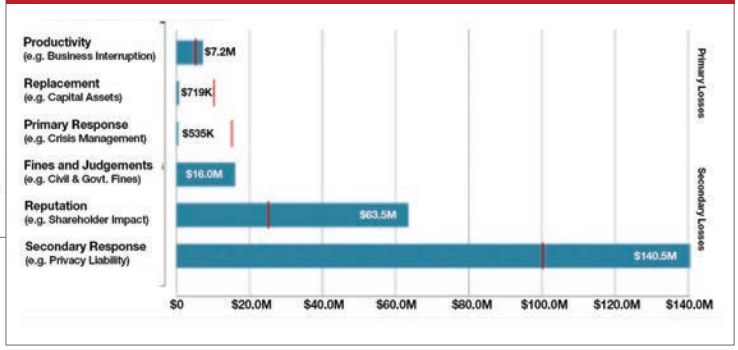
These comparisons can be made based on averages or other points within the loss exposure distribution (e.g., the tails). The charts below provide examples of this sort of comparison, which can guide decisions regarding where to focus risk management efforts.

WHAT ARE OUR TOP RISKS?



SOURCE: RISKLENS.COM

WHAT TYPE OF LOSS CAN WE EXPECT?



SOURCE: RISKLENS.COM

HAVE WE REDUCED RISK?

SOURCE: RISKLENS.COM

Once an organization is able to focus on where to concentrate their risk management efforts, it can then evaluate the value proposition of its risk reduction options and conduct cost-benefit analysis by comparing the cost of each option to the risk reduction potential.

Choosing between solution options through cost-benefit analysis is just one of several what-if use-cases for risk analysis. For example, you might also want to understand how much more risk is likely to exist if the threat landscape changes in some fashion, if the organization adds a whole new set of technologies, or if it acquires another organization.

Or perhaps there's a question about how much and what type of cyber insurance the organization needs. These use-cases all are easily within reach of a good quantitative risk analysis solution such as RiskLens.

Minimizing Effort

Many people believe developing the formulas that underly quantitative analysis is the hard part of application development. In truth, the more difficult aspect is creating a user environment that is easy to use, flexible and efficient. Furthermore, minimizing user effort applies to multiple dimensions of the user interface — setup and configuration of the application; defining the scenarios to be analyzed; entering data; and reporting analysis results.

Just a few examples of the RiskLens features that help to minimize user effort today, include:

- Configuration options that align reporting with geographic, business structure, business process or other organizational considerations
- Libraries for assets, loss tables, threat communities and controls
- A simple step-by-step point and click interface for scoping analyses
- Streamlining data reuse and multiple what-if analyses by allowing users to copy and repurpose previously completed analyses
- Enabling quick-and-dirty analyses using a triage tool

It has taken years of in-the-trenches use and user feedback to evolve the RiskLens interface to its current state of efficiency. Needless to say, that process will continue indefinitely.

Beyond the Basics

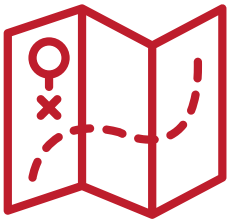
Once the foundational analytic, reporting and user needs were met, the power and utility of the application was expanded to include capabilities, such as:

- Aggregating risk across many scenarios (portfolio analysis)
- Tracking and reporting changes in aggregate risk over time
- Sensitivity analysis for massive what-if evaluations
- The ability to define and report against a clearly defined quantitative risk appetite
- An API to support pushing and pulling data to other technologies like GRC tools

Moreover, the application's capabilities are continuously being extended and evolved based on customer feedback and innovations developed within RiskLens.

CHAPTER 7

Building Successful Quantitative Risk Management in Your Company



The Roadmap to Success— and Some Common Obstacles

It's one thing to recognize the need for more mature risk measurement, and altogether another to operationalize it successfully in your organization. In this chapter, we'll briefly touch on some of the potential obstacles to success. After that, we'll provide a high-level adoption roadmap that has a track record of helping organizations transition to these methods successfully.

Common Obstacles

Introducing change within any organization can be tough. There often are cultural challenges, egos to manage, well-ensconced processes to change, skills gaps to fill and sometimes even external pressures (e.g., regulatory and industry standards) to deal with. Trying to build a quantitative risk management program very often also means overcoming misperceptions and ignorance about quantitative methods.

The roadmap section, below, describes steps that have been effective at overcoming these challenges.

A Roadmap to Success

Despite cultural and operational differences between industries and organizations, there appear to be some fundamental steps that consistently help to smooth the process of building quantitative risk management programs.

Name Your Pain

This step should almost always come first. Few organizations are going to endure the pain of change unless they have a reasonably clear understanding of "Why?"

The "Why?" will vary from organization to organization, but some of the most common reasons we see are:

- Boards of directors or senior executives are weary of heat maps and other vague sources of risk intelligence. They want to understand cyber risk in financial terms and ensure business-aligned decisions are made regarding budgeting, prioritization, resource allocation, etc.
- The organization is drowning in "high risk" conditions that everyone's intuition recognizes doesn't reflect reality. They know they need to fix the signal-to-noise problem, but don't know how.
- Regulators have raised the bar in terms of their expectations. They want more rigor and justification for the things that are, and aren't, getting done.
- The CISO wants to even the playing field when fighting for budget dollars by better articulating the value of cyber security.

Socialization

The only thing less welcome than change itself is unexpected change. As a result, it is crucial to socialize the proposed changes and the reasons for those changes with key stakeholders at all levels of the food chain.

Build a Coalition

It can be a lonely and frustrating slog trying to introduce this kind of initiative by yourself. Getting the support of both peers and those above you in the food chain can make a huge difference in the odds of success and the level of difficulty you face. One potential ally should be your colleagues within the enterprise risk management organization (if that exists where you work). Aligning your efforts with theirs can simplify the adoption path.

Training

Very few organizations have qualified staff dedicated to performing risk analysis. Unfortunately, analysis doesn't happen on its own, and poorly done analyses can not only result in bad decisions but they also can cripple the overall effort. Personnel performing risk analysis must be well trained. Note that it sometimes makes sense to bridge the skills gap using expert professional services.

Quick Wins

Being able to quickly demonstrate the value of sophisticated risk measurement can help jumpstart a program. Conversely, momentum and support can die on the vine if it takes too long to see results. The key is to not boil the ocean out of the gate. Solve relatively simple (but important!) problems early on, and get results in front of executives sooner rather than later.

Process Integration

Long term success depends on integrating mature risk measurement into operational processes. Once the organization is used to making better informed decisions on a regular basis, it won't want to revert to "the old ways."

Examples include, but aren't limited to:

- Audit finding analysis
- Policy exception management
- Change management approvals
- Project management
- Third-party risk management

Strategic Application

Top 10 risk identification; enterprise-wide risk portfolio management; tracking and trending aggregate risk over time; and managing risk against a clearly defined risk appetite are all examples of strategic opportunities where quantitative risk measurement can make a big difference. There is no other way to achieve these objectives than through quantitative risk measurement.

Although this is the recommended recipe for success, we've seen organizations be successful without following this. One very large organization started out by going straight to identifying its top-10 risks, which was a two to three month process. The keys to that organization's success included the fact that it was being driven hard by senior executives to answer to these questions, and they filled the skills gap with FAIR-certified professional services. The advantage they had after completing the process was that any opposition to change had pretty much vanished, and there was no going back to old ways.

There are a couple of considerations the roadmap doesn't account for:

- Many members of the risk management industry tend to gravitate to common practices by default (think: safety in numbers). With that in mind, we're seeing fewer intense objections to quantitative risk management approaches as adoption grows. At some point, these mature methods will become mainstream and any organization not following them will be viewed as deficient.
- There is an active and rapidly growing global FAIR community and ecosystem that is leading the way. In order to leverage this, we strongly encourage you to join the FAIR Institute, an expert non-profit organization of executives and practitioners dedicated to helping the industry evolve its risk management methods.

Visit www.fairinstitute.org or more information.

Wrapping Up

Here's What it All Boils Down to:

Many organizations place significant emphasis on compliance levels, maturity scales and benchmarking against others within their industry. Reliance on these measurements stems primarily from an inability to measure risk accurately in business terms. What does this mean for organizations today? The vast majority of them are unable to reliably identify and focus on their most important cyber risks in the most cost-effective manner.

Challenges

There are a handful of foundational problems that prevent organizations from measuring risk accurately and reliably. These are neither inherently difficult or costly to fix, but there are challenges — e.g., reliance on outdated conventions, misperceptions about risk measurement and good old-fashioned resistance to change.

Qualitative vs. Quantitative

Although useful to a degree, qualitative risk measurements (high/medium/low, etc.) have important limitations in terms of prioritizing effectively. They also are next to useless for understanding the cost-benefit proposition of risk management activities or technologies.

Done correctly, quantitative risk measurements expressed in probabilistic and economic terms enable organizations to reliably focus on the things that matter most. They also support meaningful cost-benefit analysis so that organizations can be cost-effective in their risk management choices.

Common Concerns

There are two primary concerns about quantitative cyber risk analysis:

1) Does enough data exist to reliably quantify cyber risk,
2) Does it require too much effort?

Fortunately, the answers to these concerns are "yes" and "no," respectively. There are plenty of technologies in the security and risk industries that provide numeric (i.e., quantitative) results. However, just because something is numeric doesn't mean that it helps solve the foundational problems of prioritization and understanding the value proposition of risk management efforts. .

A Proven Solution

Organizations can both improve their qualitative risk measurements and pragmatically perform quantitative risk measurements using an open, international standard for risk measurement, such as Factor Analysis of Information Risk (FAIR). FAIR has a global and rapidly expanding user base from organizations of all sizes, across all industries.

RiskLens offers a pragmatic, enterprise-class software solution purpose-built on FAIR to improve the efficiency and power of quantitative risk analysis.

To learn more, read our FAIR FAQ. (www.fairinstitute.org/frequently-asked-questions)

Resources

Detailed information about FAIR and how to apply it to support well-informed decision-making can be found in these resources:

Measuring and Managing Information Risk: A FAIR Approach. (Jack Jones and Jack Freund). Available on amazon.com (http://amzn.to/2pXshs0) in both softcover and electronic form.

Risk Taxonomy. Available from The Open Group online, here. (https://www2.opengroup.org/ogsys/catalog/C13K)

The FAIR Institute blog, resources and events. For more information, visit www.fairinstitute.org/blog

RiskLens, the leading provider of cyber risk quantification solutions built on the FAIR method. For more information, visit www.risklens.com.