RSA

3 ESSENTIALS FOR CYBER RISK QUANTIFICATION

BUSINESS-DRIVEN SECURITY™ SOLUTIONS

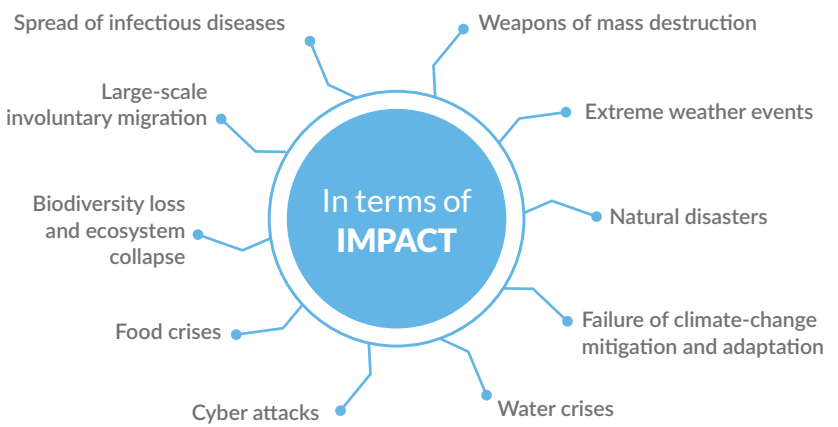
ACCURATE CYBER RISK MEASUREMENT MATTERS. HERE'S WHY.

The need to manage cyber risk is more pressing than ever. According to the World Economic Forum's The Global Risks Report 2018, cyber attacks rank No. 3 among the top ten risks for businesses in terms of likelihood, outranked only by extreme weather events and natural disasters. In terms of impact, cyber attacks didn't even make the list in 2017—but now they're listed at No. 6.

As cyber risk grows, so does the need to quantify it. If you can't quantify risk, how can you calculate how much cyber insurance you need? Or prioritize investments in security controls based on where you see the most risk? Or calculate the return on those investments?

The good news is you *can* quantify cyber risk. Read on to learn more about three ways to make cyber risk more measurable for your organization.

TOP TEN GLOBAL RISKS 2018



Source: *Based on information from World Economic Forum Global Risks Perception Survey 2017-2018*

BENEFITS OF QUANTIFYING CYBER RISK

UNDERSTANDING THE BUSINESS IMPACT OF RISK:

Quantification of cyber risk makes it possible to see risk in terms of its potential business impact on customer base, share price and other typical measures of business value.

PRIORITIZATION OF RISKS AND CONTROLS:

Effective cyber risk management depends on being able to identify and focus on the most critical risks, i.e., those that are most likely to occur and to have the greatest impact.

ACCURATE RISK ANALYSIS:

Cyber risk quantification is a valuable tool for a variety of risk analysis scenarios, from performing cost-benefit evaluations on risk treatments to calculating the effects of technology or business changes on the organization's risk profile.

1 DEFINE RISK PRECISELY

A fundamental problem with many methods for measuring cyber risk today is that they use basic terms like "risk" and "threat" imprecisely and inconsistently. This makes it difficult to measure risk reliably or communicate about it effectively.

The FAIR Institute, which promotes the Factor Analysis of Information Risk (FAIR) framework for measuring cyber risk, argues for defining risk more precisely by viewing it in terms of potential loss events—for example, a malicious breach of sensitive consumer or corporate information, cyber theft of intellectual property or destruction of critical data.[1]

These specific loss-event scenarios differ significantly from more general descriptions of risk, such as "weak passwords," "cybercrime" or "disgruntled former employees," which are really more accurately described as factors that contribute to risk. Loss events can be assessed in concrete terms, such as frequency (how likely they are to happen) and magnitude (how much impact they may have), which in turn makes it possible to measure risk more accurately and communicate about it more clearly.

TERMINOLOGY FOR DEFINING CYBER RISKS:

Based on A Clarification of "Risks"? white paper, the FAIR Institute[2]

[1] World Economic Forum, The Global Risks Report 2018

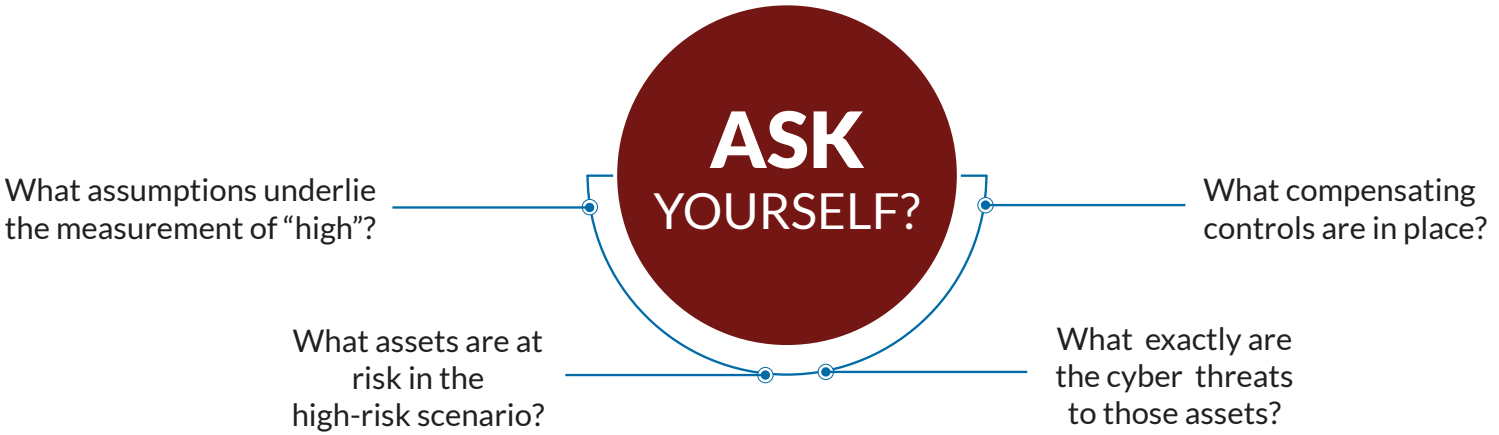
[2] Jack Jones, "A Clarification of 'Risks'?", written for the FAIR Institute Cyber Risk Management Workgroup, January 2017

2 SCOPE RISK CLEARLY

Many frameworks for defining or measuring cyber risk today assign risk ratings of high, medium or low (often designated by color, i.e., red, yellow or green). That may seem sensible. But unless you know the underlying assumptions about those categories, you can't really understand the true scope of the risk.

For example, when you say "high-risk," what do you mean by "high"? It is, after all, a relative term: Knee-high to a grasshopper is something entirely different than high as the moon. So if you use the term without context, you don't really have an understanding of what you're measuring.

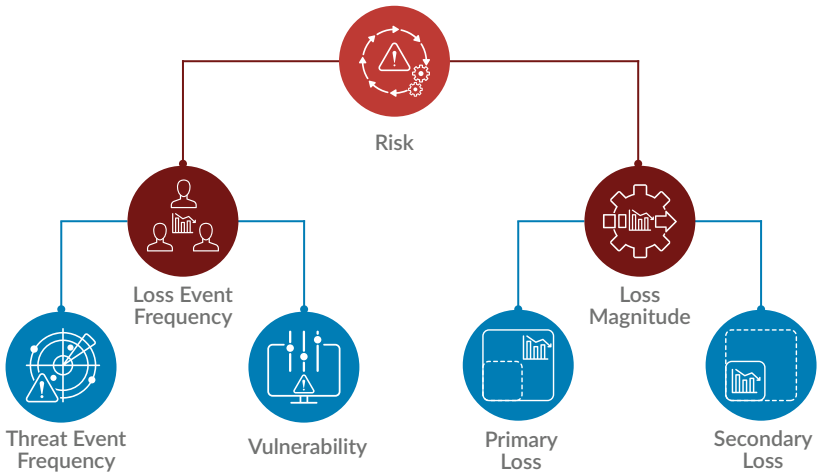
The next time you hear something described as posing a high risk, ask yourself:



3 APPLY ACCURATE MODELING

The quality of cyber risk measurement today often depends on how well the practitioners measuring the risk understand the complex array of factors in play. Cyber risk measurement is a fairly new discipline, and it shouldn't be surprising that few cybersecurity professionals are trained in its principles. Combine the lack of skills, training and experience with the previously described problems of imprecise terminology and inaccurate scope, and you're not likely to end up with an accurate model for measuring cyber risk.

FACTOR ANALYSIS OF INFORMATION RISK (FAIR)



The FAIR Model for Risk Measurement

To measure cyber risk accurately, you need a new, more effective model for quantifying risk. Factor Analysis of Information Risk (FAIR) is an open international standard risk model that was developed specifically to enable effective risk measurement. At its core, FAIR is a risk calculation model that overcomes issues of imprecision and lack of scope by specifically taking into account loss events, their likelihood and their magnitude.

FAIR addresses several of the shortcomings of existing approaches to risk measurement in the following ways:

- Defines risk factors clearly and completely to reduce imprecision and confusion
- Takes into account the mental models of those tasked with measuring risk to help ensure accurate scoping and measurement
- Provides a framework for critical thinking to lessen the chance of overlooking key factors
- Enables robust quantitative analysis using established methods
- Can be applied using a triage approach to quickly establish priorities for risk treatment or as part of a more in-depth, long-term risk management plan

RSA CYBER RISK QUANTIFICATION

RSA Archer Cyber Risk Quantification quantifies an organization's financial risk exposure to cybersecurity events, utilizing a purpose-built platform that leverages the Factor Analysis of Information Risk (FAIR) methodology. This use case under the RSA Archer IT & Security Risk Management solution area provides a set of modular applications to help organizations get started quickly quantifying cyber risk in financial terms, including mathematical simulations to a build a risk profile with limited data. It enables businesses to quantify and communicate their cyber risk in the standard business language of money. Armed with the understanding of cyber risk in financial terms, the business can calculate and demonstrate the value of cybersecurity initiatives.

For more information about RSA Archer Cyber Risk Quantification click here

ABOUT RSA

RSA® Business-Driven Security™ solutions uniquely link business context with security incidents to help organizations manage digital risk and protect what matters most. With award-winning cybersecurity solutions from RSA, a Dell Technologies business, organizations can detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud and cybercrime. RSA solutions protect millions of users around the world and help more than 90 percent of Fortune 500 companies take command of their security posture and thrive in an uncertain, high-risk world. For more information, visit rsa.com.

04/18, Ebook, H17094.