Rethinking Cybervalue at Risk
A Practical Case for Risk Quantification

Cyberrisk is a universal issue. The trustworthiness of various risk assessment methods in pursuit of risk-based decisions is largely questioned in the marketplace. At one point in recent history, subjective risk analysis techniques were the leading practice. Today, decision makers rarely choose a course of action without clear sight of the value at risk and the return on risk investments. The demand for these objective approaches is prevalent not only because of the ability to synthesize risk exposures in financial terms, but also to deliver a clear message that can be conceived by business participants. More recently, with heightened awareness of cyberrisk, organizations are shifting their attention from subjective to objective risk analysis techniques through risk quantification; however, with the convoluted digital landscape and the scenarios it presents, the pursuit of objective risk analysis is not always straightforward.

This article reviews risk management trends in light of the evolving business landscape. It also outlines what to expect of quantitative risk analysis and arms businesses to perfect the art of risk quantification by providing practical insights for modeling objective risk analysis.

Emerging Risk Management Trends

Business and user communities are evolving at a pace that has not been witnessed before. Ironically, it is sometimes argued that technology and society are evolving faster than businesses can naturally adapt. This trend, in all likelihood, may continue and intensify in magnitude in the future. This scenario means that it is fundamental for an organization to objectively make risk-based decisions in a dynamic fashion that adequately accounts for the key influences that contribute to the risk exposure of its undertakings. A plethora of frameworks (such as *COBIT® 5 for Risk*,[1] the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC)'s ISO/IEC 27005,[2] US National Institute of Standards and Technology [NIST]'s Special Publication [SP] 800-30,[3] OCTAVE,[4] and Open Web Application Security Project [OWASP])[5] provide guidance on carrying out risk analysis. While the majority of these frameworks converge on the common lineages for risk analysis, the beliefs that forge them vary largely with user interpretations. User interpretation makes some of these frameworks either outwardly simple or overly complicated, and the frameworks' suitability is often debated, i.e., if a given framework is best for data novices or data scientists. This criticism is not associated with any particular framework itself, but with the shortcomings in how it is applied to inform target audiences of risk exposure.

The following list summarizes representative operational shortcomings, which have no bearing on the previously mentioned frameworks:

- **Uneven contours of risk scoring methods**—The use of ordinal scales (high, medium, low), while having contributed as a meaningful index of risk exposure in the past, has been a nightmare to interpret for decision makers, cross-functional units and organizational entities.
- **Inconsistent and/or incompatible risk scales**—The nonhomogeneity of the risk scores (i.e., they could be on a scale of one to three, one to five or one to 10) across an organization poses considerable complexity in understanding the real risk among users. It is not uncommon to encounter situations in which a rating that is considered high in one part of the organization is considered medium in another part of the organization.
- **Misconceptions of data as a result of cognitive disparities**—Sometimes the lack of a structured decision analysis process negatively influences the outcomes of risk analysis. Human bias often becomes the weakest link in the risk analysis process for many organizations due to diverging

Sudhakar Sathiyamurthy, CISA, CRISC, CGEIT, CIPP, ITIL Expert
Is a director with Grant Thornton's risk advisory services, focusing on cyberrisk. His experience has been shaped by the opportunity to help clients design and implement strategies to achieve a risk-intelligent posture. Sathiyamurthy frequently advises clients on standing up and scaling cyberrisk capabilities and benchmarking them against laws, regulations, leading practices and industry standards. He has contributed to various cyberrisk innovation efforts and authored points of view and articles for leading journals. Sathiyamurthy can be contacted at sudsathiyam@gmail.com.

focus, and it often leads to a lack of confidence in the overall risk-based decision.

- **Obsession with data**—The biggest challenge of risk analysis, as it is with any analysis, is the ability to engender meaningful insights from data. While the quality and trustworthiness of upstream data are going to play a pivotal role in the overall risk calculations, sometimes the most meaningful insights come from common sense rather than dependence solely on data.

> **"Deterministic risk analysis is often person or occasion dependent, hence, it is often referred to as risk discerned through feelings."**

- **Measuring too much, too soon; measuring too little, too late**—Successfully conducting an objective risk analysis, for the most part, will not provide results instantaneously. Changes to the risk-assessable universe (e.g., business processes, applications, infrastructure, facilities, vendors, scenarios and projects), the volume and quality of intake data (e.g., empirical data, market data or specialist judgments), and the level of confidence in the model used can have incredible implications. It is not uncommon to find risk analysis with a significant number of uncertain inputs, regardless of their relevance to decision making.

What to Expect of Quantitative Risk Analysis

There has been extensive debate on the use of quantitative models in the past and, until now, the hesitancy to adopt these models has resulted from limitations of empirical data, complexity of frameworks, reliability of statistical models/ mathematical principles and the lack of stakeholder confidence, to name a few factors.

Why is it a challenge to adopt quantitative models? First and foremost, most quantitative risk models operate on a probabilistic approach and end users are not quite used to it. Unlike point or single estimation methods, which are deterministic in nature, quantitative models are stochastic or simulative in nature where estimates are probability distributions of potential outcomes. Deterministic risk analysis is often person or occasion dependent; hence, it is often referred to as risk discerned through feelings. Some fundamental factors that back a cyberrisk model naturally follow the most probable circumstances, and the use of probabilistic methods increases the statistical significance and reliability of analysis. Statistical methods, such as Monte Carlo (a computational model used to solve a problem that has a probabilistic interpretation), are widely in use to synthesize the randomness of the samples and generate probable distributions. Like any forecasting method, the model will be only as good as the probability estimates the user makes, i.e., an uninformed user making an erroneous estimation defeats the purpose of the analysis.

Second, quantitative risk analysis models are multifactorial and integrate data points from factors such as threats, vulnerabilities, criticalities and magnitude of loss of the risk-assessable universe for arriving at the risk exposure. An illustration of key factors that contribute to risk analysis is depicted in **figure 1**.

The multifactorial data fusion transpires beyond the mechanics or calculation and necessitates a cultural harmony between the functions that source the data. A lack of coordination and teamwork is one of the lingering bottlenecks for quantitative risk programs to be effective.

Third, data alone do not deliver actionable intelligence. Sometimes it is easy to let the data speak on their own. However, what if the data tend to deceive and confuse audiences? A raw outcome from quantitative risk analysis without interpretation is not of much value. Sometimes, the density of statistical analysis can confuse end users who are conditioned to review risk as patterns

Figure 1—Piecing the Risk Puzzle Together

of colors (e.g., red, amber, green color coding), as opposed to statistical figures. User experience is the cornerstone and also the reason that many quantitative programs fail. The raw data need to be harnessed to the degree that they can be insightful for decision-making purposes—a top-down and bottom-up understanding of the goals that influence decisions can help align data enrichment expectations and improve usability.

Other challenges that are more organizational in nature include marked shortages of true cyberrisk skills to build and operate the quantitative cyberrisk program. Qualified talent with necessary skills is in extremely short supply.[6]

Some of these challenges simply cannot be ignored. But when used properly, quantitative models can offer insightful analysis that accounts for some of the verified mathematical principles that have been and are used extensively across different business disciplines.

Nevertheless, realizing the value of risk quantification requires a strong reinforcement of the previously articulated facts and reflections from the marketplace as well as an intelligently formulated viewpoint of standing up a quantitative model. The key value drivers of quantitative risk analysis are summarized in **figure 2**.

Arming Businesses to Cope and Thrive With Quantitative Risk Analysis

Before beginning the quantitative risk analysis journey, ask the following questions, at a minimum:

- What actions should be inspired through quantitative risk analysis? Does the quantitative model reflect this message?
- Who are the audiences, and how technical are they (e.g., data novices vs. data scientists)?
- Will the message come across in the risk analysis as percentages or absolute values? What do the data mean to audiences? Are the data understandable?

Figure 2—Business Value Drivers for Embracing Quantitative Risk Analysis

> **Quantitative risk analysis requires the right intellectual capital, carefully selected cross-functional teams and partnerships, and a supportive corporate culture.**

- Which automation use cases are likely to drive value?
- How should the outcome of risk analysis (composition, comparison or distribution) be presented?

Quantitative risk analysis is not just a plug-and-play model; it is an integrated play among the governance, process and technology constituencies. **Figure 3** shows the conceptual quantitative risk analysis model that links governance, process and technology.

Governance

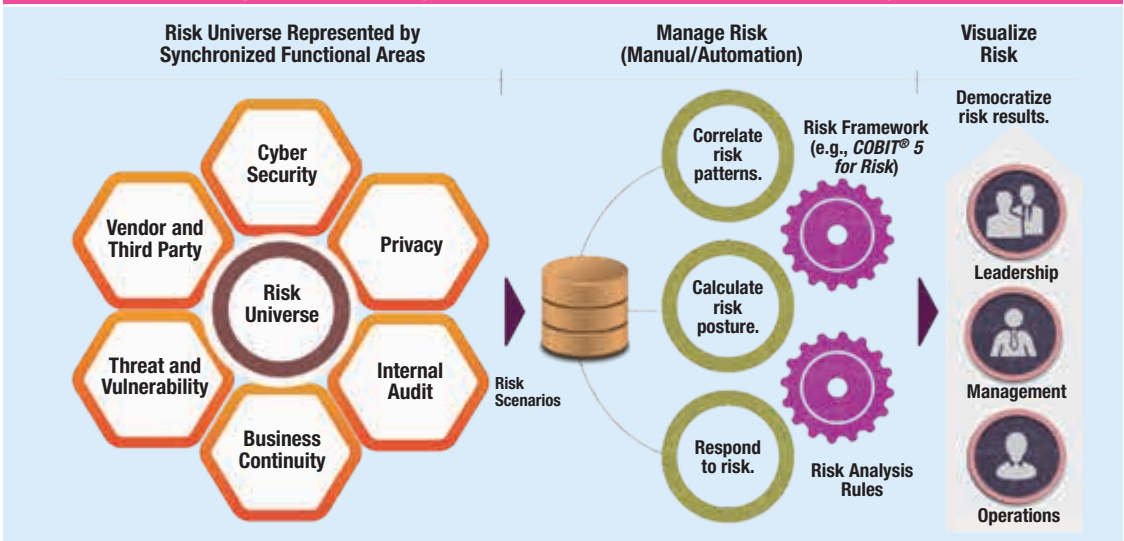
Without the right people, the quantitative risk analysis paradigm cannot grow and it certainly makes it difficult to sustain momentum over time. Quantitative risk analysis requires the right intellectual capital, carefully selected cross-functional teams and partnerships, and a supportive corporate culture that can help orient the teams and make the paradigm stick.

Consider a recent case study on super-recognizer detectives.[7] Super-recognizers are characterized by remarkable cognitive ability to register and mentally map facial features of an adversary and correlate them in any given state of play. The ability to never forget a face is an innate skill and is an inspired revolution in policing. Drawing a parallel with the psychology for risk practitioners, acquiring the traits of super-recognizers will certainly benefit in sensing key risk factors; however, these traits require a high degree of coordinated expertise and might not be likely without an integrated governance process. Such an integrated play within an organization does not happen in a vacuum and has to be better managed through cultivating cyberrisk talents, nurturing behavioral changes and composing a harmonious play between various functions.

Process

As noted previously, the quantitative model will be only as good as the estimates the user makes. The glaring and most often ignored bottleneck relates to some of the fallen risk fundamentals. For example, the inconsistency in the use of the term "probability" between different users within an organization might create profound adverse effects on the outcome of risk analysis. Probability-related terms, such as

Figure 3—Linking Governance, Process and Technology



"possibility," "likely," "unlikely" and "rarely," muddle the genesis of estimation. Human cognitive biases of these words diminish the level of confidence in analyzing the real probability. Remember the common probability debates on tossing a coin or rolling a dice? All of these calculations demand a synchronous understanding of quantitative models themselves. Risk should be ascertained not just by feelings, as flawed interpretations lead to bad decisions, and bad decisions lead to adverse outcomes (such as diminishing returns on cyberrisk investments).

One other glaring problem often noted is the chance of theoretical influences overshadowing the pursuit of organizations' mission to objectively assess risk factors, which is why it is highly recommended that organizations consciously stay connected to their primary values rather than being sidetracked. Remember, it is important to nail down the risk model; however, knowing what the relevant risk scenarios are is far more important.

Technology

The historical use of silo technologies with inherent limitations to handshake with enterprise solutions and autonomous functional camps bingeing on point solutions led to automation fatigue in some organizations.

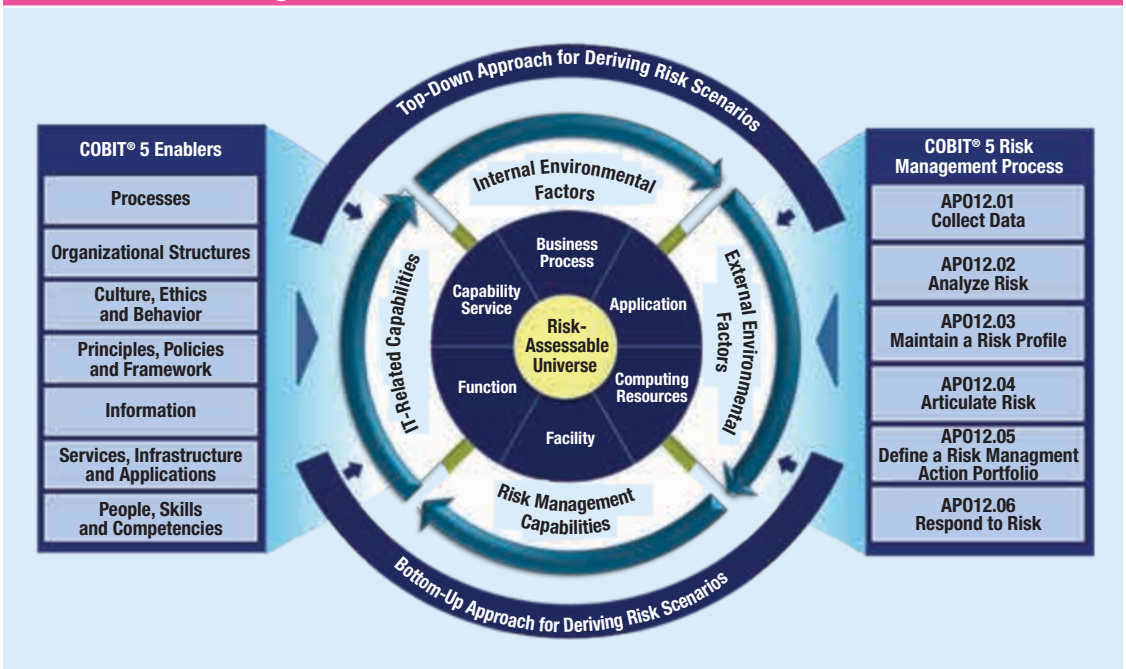
In many respects, laying the infrastructure for quantitative risk analysis is more like creating a fine clock—the simple expectation is to keep the clock ticking along, as a perfect machine, and to get the time right. In summary, the business value of the clock outpaces the fancy inner structures. Drawing a parallel to risk technologies, the expectation of the technology is to fulfil the business value by providing accurate, credible and timely intelligence of risk, rather than getting tangled in solution warfare.

In the context of usability, it is not uncommon for even well-planned risk technologies to fail due to shortfalls in user experience. Because the quantitative risk analysis model will be serving the demands of a large user base, driving increased value depends on technologies operating in novel ways to respond to consumer demands. Consumer-friendly technologies focus on transparent and trustworthy features that empower users.

Where to Get Started?

An illustration of modeling a quantitative risk analysis approach using *COBIT® 5 for Risk* as an example is illustrated in **figure 4**. The key enablers and processes support the conduct

Figure 4—Illustrative Features of *COBIT®5 for Risk*



Enjoying this article?

Enjoying this article?

- **Read *Risk Scenarios Using COBIT® 5 for Risk.*** *www.isaca.org/riskscenarios*
- **Learn more about, discuss and collaborate on risk management in the Knowledge Center.** *www.isaca.org/risk-management*

> **"The characterization of assets is the bedrock of intelligent risk analysis and enables an organization to gain better control of its assets."**

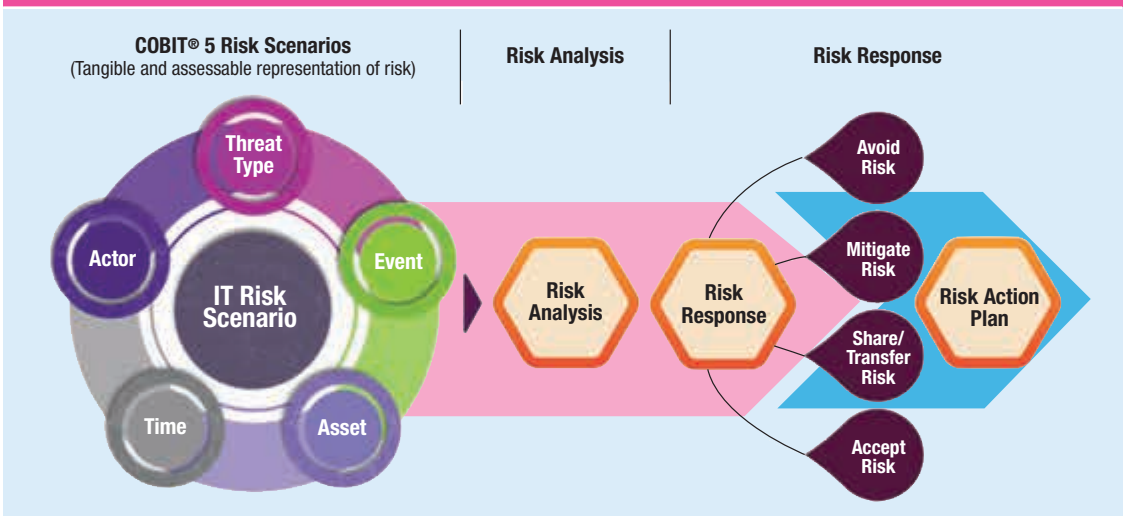
of risk governance and management within an organization. The framework also offers distinctive, but complementary mechanisms for selecting risk scenarios based on top-down and bottom-up approaches, indicated as underlying forces in **figure 4**. The risk scenarios are tangible and assessable representations of risk and account for the risk-assessable universe and the underlying threat actor, motive and outcome. The risk factors (internal environmental factors, external environmental factors, risk management capabilities and IT-related capabilities) influence the frequency and/or business impact of the risk scenarios. In this sense, the risk factors play a significant role in risk analysis.

Every organization's risk analysis journey will be different. Recognizing that a one-size-fits-all approach is seldom appropriate from a risk analysis context, the selection of quantitative risk approach and computation methods should be carefully examined to match the organizational undercurrents. With that said, the approach that follows is a simple, no-regrets illustration of quantitative risk analysis. The illustration in **figure 5** orients to *COBIT 5 for Risk* processes from a directional standpoint and references one or more frameworks for risk analysis to illustrate the art of possibilities.

The most important step when starting a risk analysis campaign is to define the risk-assessable universe, which involves identifying the crown-jewel assets on which the analysis might be performed. The characterization of assets is the bedrock of intelligent risk analysis and enables an organization to gain better control of its assets. Depending on the level of abstraction, the risk-assessable universe can be as broad as an organizational entity or as atomic as an application or a system.

With the risk-assessable universe firmly in place, the next important step is to ascertain the risk scenarios that are relevant to an organization. The selection of risk scenarios should sensibly account for the components (actor, threat type, event, asset and time/duration of impact) referenced in **figure 5**. Focusing on relevance over perfection while

Figure 5—Conceptual Model Outlining the Risk Analysis Integrating *COBIT® 5 for Risk* Scenarios



selecting the risk scenarios is critical to success. *COBIT® 5 for Risk* offers generic risk scenarios grouped under 20 risk scenario categories, which might serve as a starting point to derive relevant and customized risk scenarios.

Conducting an objective analysis of the risk scenario is not possible without analyzing the underlying threats, vulnerabilities and assets. Various industry models and frameworks offer approaches to statistically analyze and derive risk quantitatively based on these three core components. The following steps summarize some of the common methods of analyzing threats, vulnerabilities and assets:

- **Review threats**—Intelligence about known attacks, adversaries and adversarial behavior is fundamental to making informed decisions on probable threats. The likelihood of a threat is typically expressed as the probable number of threat events, and the capability of threat is typically expressed as a percentage.

  Where to start? The OWASP model helps in estimating the likelihood of threats based on factors such as skill level, motive, opportunity and size. Another model of evaluating threats is based on damage potential, reproducibility, exploitability, affected users and discoverability (DREAD).

- **Review vulnerabilities**—It is critical to have a resilient design and operation of baseline controls for constraining the systemic risk posed by threats commensurate to an organization's structure, complexity and size. Vulnerability is usually a point-in-time depiction and might increase or decrease in concentration based on inherent and emergent weakness to controls, or due to the fluctuating capability of threat. Vulnerability is typically expressed as a percentage strength of baseline controls to thwart the threat.

  Where to start? The Common Vulnerability Scoring System helps to characterize the vulnerability based on base, temporal and environmental metrics. The OWASP model helps in analyzing the vulnerabilities based on factors such as ease of discovery, ease of exploit, awareness and intrusion detection.

> **"Perfecting the art of risk quantification is about staying real and relevant to the outcome and the business value drivers of risk analysis."**

- **Review asset impacted**—The potential impact of an asset denotes the value and the liability it presents to an organization. Conversely, the degree of impact affects each asset differently and is driven largely by the asset value and liability. From a risk scenario connotation, impact is the probable loss exercised on an asset when the threat is realized. Impact is typically expressed in financial terms.

  Where to start?—The OCTAVE Allegro model offers risk measurement criteria to analyze the effects of a realized risk based on factors such as reputation/customer confidence, financial, productivity, safety and health, and fines/legal penalties. The OWASP model helps estimate the impact using technical impact factors such as loss of confidentiality, integrity, availability and accountability, and business impact factors such as financial damage, reputation damage, noncompliance and privacy violations.

In the previously described analysis, whenever the outcome is probabilistic, statistical models such as Monte Carlo computations might help to analyze the best-case, most-likely-case and worst-case estimates for quantitative processing.

Perfecting the Art of Risk Quantification

Perfecting the art of risk quantification is about staying real and relevant to the outcome and the business value drivers of risk analysis. In an ecosystem that is characterized by an overabundance of data, the quest for objective decision making is fairly natural. Paradoxically,

even with the extraordinary access to big data, organizations struggle to get a better sense of the uncertainties and the risk that exist. The reality often indicates disproportionate concerns faced by governance, process and technology constituencies within an organization. While the weak spot for most risk quantification undertakings is a chronically complex vision, emphasizing a defensible and usable strategy helps to create practical models and revive objective risk analysis. The key takeaway is to make the risk philosophy stick, which is achievable by being smart about modeling and integrating quantitative risk principles into design, build and operations. Organizations that understand effective risk quantification continue to set the pace for other organizations and garner profound effects through sensing and synthesizing accurate, credible and timely risk intelligence.

Endnotes

1 ISACA®, *COBIT® 5 for Risk,* USA, 2013, *www.isaca.org/cobit5*
2 International Organization for Standardization/ International Electrotechnical Commission, ISO/IEC 27005:201, *Information technology—Security techniques—Information security risk management*, *www.iso.org/iso/catalogue_detail?csnumber=56742*
3 National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, SP 800-30, USA, September 2012, *http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf*
4 Software Engineering Institute, *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, May 2007, *www.cert.org/resilience/products-services/octave*
5 Open Web Application Security Project, *https://www.owasp.org/*
6 *ISACA, State of Cyber Security 2017*, USA, 2017, *www.isaca.org/Knowledge-Center/Research/Documents/state-of-cybersecurity-2017_res_eng_0217.pdf*
7 Brodwin, E.; "Meet the 'Super-recognizers,' an Elite Squad of Police Officers Who Are Paid to Never Forget a Face," *Business Insider*, 11 October 2016, *www.businessinsider.com/london-police-super-recognisers-id-faces-surveillance-2016-10*