Managing Risk at the Speed of Change

A New Risk Vocabulary and a Call to the Profession

By Sridhar Ramamoorti, Dorsey L. Baskin, Jr., Barry J. Epstein, and James Wanserski

Electronic commerce has changed the pace of business activity. One McKinsey estimate speculates that the current rate of change is 10 times that of the Industrial Revolution, and that change is happening at 300 times the scale and with roughly 3,000 times the impact (James Manyika, Michael Chui, Jacques Bughin, Richard Sobbs, Peter Bisson, and Alex Marrs, *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy,* McKinsey and Company, 2013, http://bit.ly/2qaJ6TE). With recent cybersecurity breaches, the rapid and devastating effects of information security risks are becoming widely understood and recognized. Business leaders and professionals have primarily focused on the speed with which a stellar reputation can vanish overnight. Although the emerging concept of risk velocity is only just gaining recognition among risk managers, its underlying principle and implications seem self-evident.

Measures of risk velocity—that is, how quickly one or more risks may adversely affect an organization and how different risks are changing in relation to others—may be more widespread than previously acknowledged (e.g., *Global Risk Management Survey: Fifth Edition – Accelerating Risk Management Practices,* Deloitte, 2007, http://bit.ly/2q9Fge7; Stephen Davis and Jon Lukomnik, "Risk Velocity, the Unknown Dimension in ERM," *ComplianceWeek*, Dec. 8, 2009, http://bit.ly/2qaF0Lq). After all, the basic risk/returns model suggests that anticipated risk is just as important as expected return in assessing a company's future performance. The authors believe that the velocity of risk (VoR) perspective should be factored into enterprise risk management (ERM) assessment and response strategies and be utilized to calibrate negative events as well as opportunities.

Both the COSO 2013 *Internal Control–Integrated Framework* and the 2016 COSO ERM exposure draft (expected to be released in mid-2017) take note of VoR. Specifically, the COSO ERM draft highlights the speed with which risk triggers and associated risks may develop:

> The severity of the risks and the frequency at which severity may change will inform how often the assessment may be triggered. For example, risks associated with changing commodity prices may need to be assessed daily, but risks

associated with changing demographics or market tastes for new products may need to be assessed only annually. (COSO ERM Exposure Draft, *Enterprise Risk Management: Aligning Risk with Strategy and Performance,* http://bit.ly/2r8rGEM)

This article describes VoR, suggests ways of modeling this concept as part of risk assessment, and uses the example of compliance with section 404 of the Sarbanes-Oxley Act (SOX) of 2002 in the context of cybersecurity risks to nudge the profession towards embracing the concept. The authors believe that doing so will ultimately enable CPAs to provide better service to clients, furnish more current, relevant, and insightful information to stakeholders, and adapt to a rapidly changing environment. This "third dimension of risk" is an idea whose time has come, and the profession needs to recognize it, understand it, and treat it as part of its standard operating procedures.

What Is Velocity of Risk?

A generally accepted definition of VoR has not yet emerged; however, Davis and Lukomnik define it as "how quickly one goes from the onset of the risk to the impact of the risk." They use the Lehman Brothers' sudden bankruptcy as an example: "In contrast, liquidity risk manifests quickly. Within a week or two, your counterparties stop dealing with you and you're out of business." Protiviti's 2016 Top Risks survey (http://www.protiviti.com/TopRisks) highlights the rapid speed of disruptive innovations or new technologies within the industry, which may outpace ability to compete or manage risk appropriately without significant changes to the business model.

In the last two decades, risk management professionals and internal auditors have become adept at measuring the likelihood and impact of individual risks. The information gathered for this purpose is then used to create heat maps allowing organizations to prioritize risks and develop appropriate response strategies (Kurt R. Reding, Paul J. Sobel, Urton L. Anderson, Michael J. Head, Sridhar Ramamoorti, Mark Salamasick, and Cris Riddle, Internal Auditing: *Assurance and Advisory Services,* third edition, IIA Research Foundation, 2013). While people tend to think in terms of a single risk, it is more realistic to contemplate risks operating in concert. Indeed, internal auditors are using the phrase "auditing at the speed of risk," to reflect their fast-paced and responsive efforts.

Certainly, the accelerating pace of change in the business world compels auditors to consider factors beyond just likelihood and impact of risk. Indeed, it poses a fundamental question: Is VoR a variable that risk management professionals and auditors have neglected to factor explicitly into their risk assessment and measurement models? Is it the third dimension of risk?

> Although the emerging concept of risk velocity is only just gaining recognition among risk managers, its underlying principle and implications seem self-evident.

Defining Risk Velocity

Velocity means how fast something is going in a particular direction. In the realm of risk management, VoR indicates how fast a risk may affect an organization. As part of risk assessment, velocity can be measured using a qualitative (i.e., high vs. low) analysis. An example of a high VoR occurred when evidence of food-borne disease at a nationally known restaurant chain became public (e.g., when fast-food chain Chipotle experienced *E. coli* bacteria infestation); events unfolded with debilitating ferocity, nearly halving the company's market capitalization almost immediately and resulting in much lower same-store sales for quarters beyond the original incident. A lower VoR example is an aging workforce with strong expertise; without a plan to replace seasoned and experienced staff, productivity could decline and institutional memory could disappear completely. Such a scenario is described in the Government Accountability Office's 2017 report on Strategic Human Capital Management within the federal government (http://bit.ly/2qd6j6g).

Other types of risks with low velocity include those that can lead to loss of market share to competitors over time, and long-term loss of reputation. Although historically characterized by low velocity, social media and the 24-hour news cycle may have increased the risk velocity of reputational risk.

The Direction of Risk

COSO's 2004 ERM draft states that the direction of risk matters; there is

"upside risk," or the chance to miss a beneficial opportunity, and "downside risk," or the chance of an adverse result. As an example of the former, consider the announcement of a government contract, wherein the window to apply, including the demonstration of vendor credentials and qualifications, represents upside risk. Missed upside opportunities constitute a serious concern. Adverse consequences resulting from downside risk events are readily understood by all. Clearly, there is asymmetry in the consideration of upside and downside risk scenarios, as predicted by prospect theory (Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, March 1979, http://bit.ly/2qAuChl).

> This "third dimension of risk" is an idea whose time has come, and the profession needs to recognize it, understand it, and treat it as part of its standard operating procedures.

Evaluating Risk Velocity: Three Models

The easiest way to factor in VoR is by making it part of the impact score. The quicker the consequences or impacts are felt, the higher the score. Other risk experts suggest including VoR in a well-defined formula used to evaluate risk scores. Two examples are worth considering:

- ***(Likelihood + Velocity) × Impact.*** Under this formula, proposed by Harry Hall on the PM South blog ("How to Evaluate Risk Velocity," Apr. 25, 2014, http://bit.ly/2qjRlcX), the qualitative rating of risk velocity and the likelihood are given equal weight, and both are multiplied by the impact to produce the overall score.
- ***(Likelihood × Impact) + Velocity.*** Here, VoR is considered separately. For example, if the likelihood and impact of a risk are both 4 on a 5×5 matrix, the initial impact score is 16. Velocity is rated by estimated time before an adverse event (e.g., hours to days, which in this hypothetical is rated 3) is added to give a total score of 19 (see Karel Simpson, "Risk Velocity," *Capable People,* Mar. 31, 2015, http://bit.ly/2pG3qsx).

In addition to these two-dimensional models, VoR can also be modeled in three dimensions, where velocity is a factor in itself, such as *Likelihood* × *Velocity* × *Impact*. Such models await further development, however, and are beyond the scope of this article.

The preference of the authors is to treat VoR as a third dimension of risk, as they believe that the speed with which one or more related risks evolve changes both their nature and scope, making them qualitatively different from other, slow-developing risks. Once this dimension is explicitly factored in, it will very likely change the risk prioritization, demanding immediate responses to fast-moving risks.

Ultimately, regardless of the approach adopted, it is important to somehow take into account how fast the impacts of risks will be felt by the organization. This will give a better assessment of risks and help prioritize risk mitigation efforts.

SOX Compliance: Risks and Response Strategies

SOX section 404 further mandates that, subject to capitalization levels, publicly traded companies must establish internal controls and procedures for financial reporting and must document, test, and maintain those controls and procedures to ensure their continued effectiveness. It also requires the company include its assessment of these internal controls in its annual report, along with an auditor's attestation.

The PCAOB's definition of internal control over financial reporting (ICFR) states that among the policies and procedures that provide reasonable assurance regarding the preparation of reliable financial statements are those that provide reasonable assurance regarding prevention, or timely detection and correction, of unauthorized acquisition, use, or disposition of the entity's assets that could have a material effect on the financial statements. From an ERM perspective, the hazards posed by cybersecurity breaches have become common. Consider the following scenarios that involve the unauthorized acquisition, use, or disposition of a company's assets:

- Through industrial espionage, a competitor obtains a company's intellectual property and begins producing and selling competing products at a lower price.
- Through hacking the company's systems, information of strategic importance is stolen (e.g., rent rolls of a commercial real estate management company).
- Through hacking of a depository institution, a group is able to trigger the

unauthorized disbursement of cash (e.g., the case of $81 million fraudulently transferred from the account of the Bangladesh Central Bank).

- Through hacking of a commercial enterprise, a group is able to prevent the enterprise from accessing and using its own systems and applications that control critical functions, causing the company to suspend operations (e.g., the "WannaCry" ransomware attack that affected 150 countries in May 2017).

From an ERM standpoint, the question is whether the procedures, policies, and internal controls in place adequately respond to, and whether the risk responses are ahead of, consistent with, or behind the velocity of, these cybersecurity risks. While cybersecurity risks are undoubtedly an ERM issue, the examples furnished are also ICFR issues in the view of some parties, consistent with the definition of ICFR cited above. In any case, the ability of cybercriminals to carry out attack scenarios is changing at different rates, which should lead entities to respond differently to different risks.

Managing Risk at the Speed of Change

Columbia University philosopher and cultural critic Mark C. Taylor presents a compelling argument tracing how speed is affecting our lives psychologically, environmentally, economically, and culturally (Mark C. Taylor, *Speed Limits: Where Time Went and Why We Have So Little Left,* 2014, Yale University Press). Certainly, global business uncertainty and complexity continue to accelerate, underscoring the cliché that "change is the only constant." In such a dynamic business environment, it is important to revisit risk-assessment models and consider the need to expand them beyond the standard, two-dimensional "likelihood/significance" representation. VoR represents a critically important dimension of risk, especially when disparate risk factors operate in concert, making risk scenarios unfold faster than expected, or when deteriorating financial conditions can precipitate the application of the "material adverse change" clause in lender financing.

Risk assessment should pay particular attention to the speed at which risks are expected to materialize (i.e., VoR), the direction of risk, and which risks may operate in concert rather than in isolation. It should be recognized that disparate risk factors, some representing negative and others representing positive potential, may occur simultaneously, and different groups within the organization may be tracking and monitoring their development. There could thus be compounding effects, as well as cancelling effects, of these myriad risk-related phenomena.

It may be worthwhile for management to actually quantify and compute some measure of the VoR and resilience, and thus improve risk calibration and response efforts. Alternatively, management should use these concepts to understand their risks and better manage them. Once incubated, a fast-moving risk tends to materialize quickly, so it is also important to recognize that resilience must be substantial. Typically, the organization's agility of response may lag behind the evolution of a cybersecurity attack, and thus be inadequate to protect the organization; instead, organizations need to follow the ideas of risk analyst Nassim Taleb *(Antifragile: Things that Gain from Disorder,* Random House, 2014) and learn to become resilient to shocks and perturbations in the environment and thus even benefit from surprise and disorder.

VoR is a foundational concept that can help organizations better manage risk at the speed of change. Risk and control professionals—whether external or internal—must think broadly about how to upgrade their risk assessment models, and auditors must devise methods of assessing whether organizations have designed and implemented appropriate response strategies—thus enabling them to better serve their clients and stakeholders in a rapidly changing world. ❑

VoR is a foundational concept that can help organizations better manage risk at the speed of change.

Sridhar Ramamoorti, PhD, CPA, CFE, CFF, MAFF, *is an associate professor in the department of accounting, school of business administration, University of Dayton, Dayton, Ohio.* ***Dorsey L. Baskin, Jr., CPA,*** *is a consultant to multiple forensic, litigation and accounting software consulting firms from Dallas, Tex.* ***Barry Jay Epstein, PhD, CPA,*** *is a principal with Epstein + Nach LLC, based in Chicago, Ill.* ***James Wanserski*** *is a principal and owner of Wanserski and Associates, Atlanta, Ga.*