RIMS
the risk management society
Executive Report

Identifying and Evaluating Emerging Risks

Identifying and Evaluating Emerging Risks

Authors

Frank Fiorille
Vice President of Risk Management,
Compliance and Data Analytics
Paychex

Lorie Graham
Chief Risk Officer and Senior Manager,
Insurance Services
American Agricultural Insurance Co.

Christy Kaufman
Risk Analytics and Insights Director,
and Chief Compliance Officer
AmFam Ventures (American Family Insurance)

Editor

Morgan O'Rourke
RIMS

Art Director

Nick Nguyen
RIMS

RIMS
the risk management society®

As the preeminent organization dedicated to educating, engaging and advocating for the global risk community, RIMS, *the* risk management society®, is a not-for-profit organization representing more than 3,500 corporate, industrial, service, nonprofit, charitable and government entities throughout the world. RIMS has a membership of approximately 10,000 risk practitioners who are located in more than 60 countries. For more information about the Society's world-leading risk management content, networking, professional development and certification opportunities, visit www.RIMS.org.

In a rapidly changing business environment characterized by advancing technology, shifting geopolitical tensions and increasing regulatory scrutiny, it is more important than ever for organizations to look beyond near-term threats to prepare for the risks they could face in the future. Broadly defined, these emerging risks are new or developing threats that have an unknown significance and impact and are therefore not well understood. Emerging risks can also be known risks that have transformed due to changes in the business environment. The key is that, even if the risk is known to some degree, the likelihood and impact of the risk is not. These "unknowns" defy traditional risk management techniques and, as a result, organizations often opt to allocate fewer resources to them. But by taking steps to identify and evaluate emerging risks, organizations can be better equipped to make important, risk-aware decisions to ensure the best long-term strategic outcomes.

The Value of Understanding Emerging Risks

The first step to identifying emerging risks is to understand the nature of the risk itself. When managing "known" risks, we generally categorize by source such as operational, financial, hazard or strategic. We understand that a structural and systematic approach to categorizing risks is helpful in identifying linkages between risks and it helps us to develop risk scenarios.

Emerging risks are unique in that they are differentiated primarily by the uncertainty about their potential probability and consequences. According to the International Risk Governance Council (IRGC) there are a three major types of emerging risks to look for:

- **High Uncertainty/Lack of Knowledge**
  Our lack of knowledge and experience with this type of emerging risk leaves us with uncertainty about how the risk may impact us and how it may interact with other known risks. These risks often arise from social or technological changes. The primary characteristic of these emerging risks is the lack of data or scientific knowledge regarding the possible impacts of the risk. Examples include nanotechnology, the sharing economy and sensor technology.
- **Growing Complexity**
  Emerging interactions and systemic dependencies can lead to surprises. These risks emerge from new interactions and adaptive behaviors. The primary characteristic of these emerging risks is deviation from known variability or a lack of awareness about how this risk interacts with other risks in a complex environment. These emerging risks can arise from the speed of innovation, changes in the regulatory environment and changes in the underlying drivers of risk.
- **Contextual Changes**
  Emerging risks can also arise from known risks where the conditions or processes that are familiar to those risks change. The potential probabilities and impacts of these previously understood risks change as the context changes. The primary characteristic is unexpected impacts from the use of an established technology or process in an evolving environment. Examples include new materials being used in an existing product, regulatory changes or economic shifts.

There are several essential reasons why organizations benefit from identifying, assessing and monitoring emerging risks.

First, it creates competitive advantage. By focusing on trends that are just beginning to surface, organizations can identify potential shifts in strategy ahead of their competitors, thereby creating "first mover" advantages.

Second, it helps "future-proof" longer-term strategies. Because strategic planning is inherently forward looking, assumptions about the future are likely to be inaccurate. The further out the planning horizon, the greater the degree of inaccuracy. Organizations that compensate for this pitfall are more likely to succeed. They do so by asking themselves:

- What future risks could impact the success of the plan?
- What are the set of circumstances or indicators that would cause us to abort, modify or double down on our strategies?
- What changes might we need to make? How and by when will we know that we need to make them?

Third, it helps minimize unwanted surprises and capitalize on opportunities. A well-developed emerging risk capability promotes early intervention. Knowing that a risk may affect goals or objectives allows companies to put plans in place to either prevent the negative effect from occurring and/or minimize the harm. It can also help them proactively plan how to use the risk for their success.

For these reasons, developing an emerging risk capability is a clear opportunity for the risk management function to add value to the organization because understanding emerging risks as they unfold can impact the success or failure of an organization. Take Sears, Roebuck and Company for example. Founded in 1886, the company prospered for over a century, becoming a leading retailer in the United States and changing the way Americans shopped. So why did this long-standing successful corporation end up filing for bankruptcy in 2011?

Over the years, several big-box competitors like Walmart and Home Depot captured a large portion of the retail market share by offering a broader array of products and better prices. As consumers started shifting to online sales, Sears did not keep up with services offered by their competitors. In 2005, Sears merged with Kmart, another declining retailer. Sears had hoped the merger would help them reduce costs and gain capital by closing the underperforming stores and selling the real estate. But Sears failed to reinvest that capital into the changing demands of their customers. Online sales have grown continuously over the past few decades. Did Sears fail to see the signs of a changing customer demographic?

Conversely, in 1994, Amazon began as an online book store. Unlike Sears, this online retailer thrived on a data-driven strategy. Amazon has proven nimble and is not hesitant to divest itself from poorly performing investments. According to Amazon founder and CEO Jeff Bezos, "Our passion for pioneering will drive us to explore narrow passages, and, unavoidably, many will turn out to be blind alleys. But—with a bit of good fortune—there will also be a few that open up into broad avenues." In order to accomplish this, Amazon uses tools like customer behavioral data to discover insights about their wants and needs. This provides Amazon with real-time perspectives on changing customer behaviors and emerging risks that lead to opportunities.

Research and Discovery

There are many sources to consider when trying to identify emerging risks. At a very basic level, you can learn a lot from news articles, professional publications and subject matter experts.

Social and cultural changes are also a source for identifying emerging risks. Trends in human behavior and demographics can provide a starting point to see how the future may unfold differently. For example, as technology advances for autonomous vehicles, consumer expectations for safety and their desire to drive will impact the adoption of this technology.

Macroeconomic changes provide insight on trends, political environment and market volatility that may impact the economy. A significant change in unemployment can have a negative or positive impact on the profitability of a line of insurance business.

Environmental changes such as climate change, can impact weather patterns, long-term viability of business decisions, and for companies that contribute to such changes, reputation.

Technology has continuously advanced at a significant rate. An organization could be blindsided by new technology or its rapid adoption. Insurtech is a recent example. In this case, non-traditional entrants into the insurance marketplace use technology to reduce costs and enhance customer experience when purchasing insurance. This technology could disrupt the insurance industry if significant market share is attainable by these technology startups. Insurtech is changing customer expectations as well, as the technology delivers speed, efficiency and personalized services.

Another area to consider is new regulations and regulatory changes. Perceptions about a particular industry could lead to new regulations for that industry. It is vital to monitor factors that could result in regulatory changes to stay ahead of the curve.

Changes in an organization's strategy can create new blind spots. As strategy changes, so does context. Keep a broad view of the emerging risks you consider, and take a look at those risks in the perspective of your organization's strategy.

Evaluating the Impact

Once an emerging risk has been identified and assessed, it is time to evaluate its potential impact on an organization. Various techniques can aid in this objective:

Scenario Analysis

A scenario analysis describes possible future situations including paths of development that may lead to those situations. It is about preparing for a variety of possible events and impacts. Organizations create and explore scenarios by asking questions like, "What would happen if...".

A scenario analysis is used to broaden perspectives, raise questions and challenge conventional thinking. The scenario planning and analysis process can be a method to communicate and promote a shared understanding of emerging risks across an organization. Organizations also use scenario analyses as a method to assist with goal setting, decision-making and strategic planning. This method can assist leaders to look for new growth opportunities in an uncertain future. By reallocating resources based on the results of a scenario analysis, an organization can more effectively prepare for emerging risks. Scenario analysis provides transparency and tangibility to the unknown risks. The greater the effort put in to exploring scenarios from different perspectives, the better understanding an organization has regarding the potential effects.

Consider technological advancements as an example. When evaluating how technology may potentially impact your organization, it is important to start by defining the scope of your analysis including the time frame and major stakeholders.

When using scenario planning for technology initiatives, an organization may consider artificial intelligence, blockchain, cyber threats, machine learning, chatbots and other new advances from an opportunity and threat perspective (Table 1).

After identifying multiple scenarios, it is important to prioritize them as well as determine which scenarios are more likely to occur and which have higher impacts. If your organization does not use or plan to use blockchain technology soon, minimal resources may need to be allocated to modify associated risks or explore related opportunities, unless this is identified as an industry trend.

Bow-Tie Diagram

Another technique that can be used to evaluate emerging risks is the bow-tie diagram, also known as a cause-and-effect diagram. This technique helps identify gaps and improvement opportunities. Cause-and-effect diagrams provide a logical, structured approach to analyzing an emerging risk. The diagram helps visualize the relationships between an emerging potential outcome and its causes and impacts by analyzing possible scenarios through simplified trees. The left side of the diagram represents the causes of the event the right side represents the effects of the event. Mapping potential scenarios for emerging risks helps to develop a deeper understanding of the risk.

Table 2 is a simplified example using the emerging trend of "abundance of data" and the potential outcome that the organization will not be able to capitalize the use of this data.

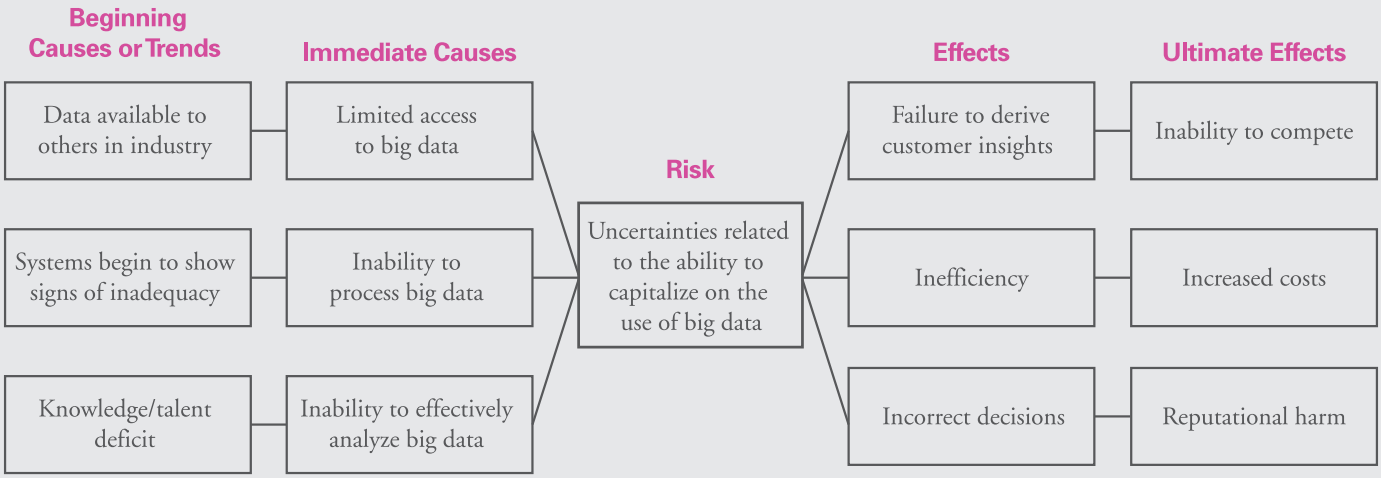
By identifying the causes, you can uncover key risk indicators that allow you to monitor the evolution of the emerging risk. Cause identification also helps you to understand where you can implement controls to prevent the risk from negatively impacting your organization.

Bow-tie diagrams are generally not linear as causes and effects are often connected. By connecting the lines, you can see where a single control may impact several drivers, where multiple drivers may act in concert, or where impacts may be multiplied.

Table 1. Scenario Examples

	Scenario A (Opportunities)	Scenario B (Threats)
AI	Increased automation leading to reduced operating costs.	Increased use of technology increases cyberthreats. The organization could fall victim to a data breach or ransomware attack.
Blockchain	Increased quality assurance due to the traceability and ability to know each entry's point of origin.	Data is not necessarily secure as blockchain is available to the public.
Chatbots	Customer service can operate 24/7. Customers can be supported instantly.	Customer satisfaction could decrease due to the limited personalization and lack of conversation.

Table 2. Bow-Tie Diagram



Delphi Technique

When there are no reliable measures or evidence, another useful method is the Delphi technique, which is used to "forecast" future events. A group of experts each independently provide estimates and assumptions to a facilitator who shares the anonymized data back out to the group, which leads them toward a conclusion. In the emerging risk context, the process works as follows:

Step 1: A facilitator sends a survey to a group of experts asking them to identify the top emerging risks for their organization. The experts provide their views to the facilitator.

Step 2: The facilitator shares an anonymous summary of the experts' risks, as well as the reasons for their views.

Step 3: The facilitator reissues the survey, encouraging the experts to revise their earlier answers in light of what they now know about other points of view. This process is repeated for as many rounds as necessary until opinions begin to converge.

Step 4: The process ceases after satisfactory achievement of consensus or some other predefined criterion, such as the number of rounds.

Once an agreed-upon universe of emerging risks has been identified, the next step is to rate them according to their plausibility. Understanding plausibility will help the organization determine which risks are most deserving of their limited risk modification resources. Considerations include:

- Impact: How might the risk affect the organization's assets, reputation and core values?
- Velocity: How quickly will the effect occur? Will it come with any warning?
- Likelihood: How likely is the risk effect to materialize? (The least emphasis is placed here, since emerging risks are, by their very nature, low frequency)

Experts can agree to these questions using the Delphi technique as well, or they can agree to them collectively in a group setting. Predefined risk rating scales can lend objectivity to the conversation.

When thinking about the priority of emerging risks, it is also important to consider their possible interaction. Perhaps a risk is insignificant in isolation, but if it has the potential to trigger several follow-on risks, it could become important. For example, consider a scenario in which increasing automation creates new IT security threats that are overlooked due to the reduction in IT personnel. A failure to adhere to IT security protocols then triggers a wide-scale breach followed by a class action lawsuit and mass client exodus. What started as an opportunity to save labor costs resulted in a massive expenditure after all the dominos fell.

After the high-priority emerging risks have been identified, the next step is to brainstorm areas of possible intervention. For each significant emerging risk, experts should consider whether there are steps that can be taken now to avoid, reduce, transfer or exploit the risk. These steps should be weighed against their relative expense and ease of implementation, especially given the high level of uncertainty around whether the risk effect will materialize. As a practical matter, it may not be possible to do anything immediately, but even having the conversation can shed valuable light on possible interventions for the future if and when the risk scenario becomes real.

Monitoring the Risk

Once an emerging risk has been identified and evaluated, it should be monitored. Key risk indicators (KRIs) are metrics related to risk exposure and demonstrate changes in the likelihood or impact of the risk occurring. KRI monitoring is often linked to an organization's risk appetite.

How an organization uses KRIs to monitor emerging risks is dependent on the risk and timing. For example, the number of cybersecurity incidents where personally identifiable information (PII) is exposed could be a KRI used to monitor cyber risk. However, KRIs likely would not be used to assess the impact and likelihood of political risks in markets that are outside the scope of an organization's strategy nor used to determine the success of a future technology innovation until the time decisions are made to move forward.

In the 2016 RIMS publication, *Emerging Risks: Anticipating Threats and Opportunities Around the Corner,* the authors found a significant aspect of emerging risks for participants was how quickly an organization is affected by an occurring risk. Known as velocity, determining how fast the risk is approaching and when it will truly have an impact on the organization is an important aspect to determine the risk management strategy. Gauging how quickly the organization will be affected by an emerging risk empowers leaders to prioritize risk management strategies such as allocating time and resources.

Risks with low velocity have a very slow onset usually happening over months or years. These risks can be monitored and assessed over time and a strategy can be formalized before implementation. Consider the process to get legislation passed in the United States. Bills must be drafted, introduced, debated and voted on. Even if passage occurs, the effective date of required action by businesses could be years from the date of signing. The velocity is slower, allowing those impacted to prepare strategies and consider possible future scenarios if the legislation is passed. Risks with a fast velocity, on the other hand, have a very rapid onset with little to no warning, requiring a different type of strategy, and a fast response.

Developing a Response Plan

A pre-emptive response plan can reduce organizational vulnerability by modifying risks, prescribing action plans and taking advantage of opportunities prior to experiencing potential effects. Plans are monitored through key risk indicators that can trigger escalation to appropriate persons when thresholds are reached. Thresholds can be tiered to respond as the emerging risk unfolds. Once these thresholds are triggered, the response plan strategy is executed. Response plans are purposefully proactive to react and adapt to changes in circumstances as they occur and build resilience for your organization.

Response plans can cover a variety of areas such as:

- Changes to strategic plans or risk appetite
- Allocation or acquisition of capital
- Alternative available resources
- Roles and responsibilities for key people
- Partnerships

They may also include traditional risk management techniques such as risk transfer and risk control.

Integrating Emerging Risks into the Known Risk Portfolio

Determining the point at which an emerging risk becomes a known risk may feel like more art than science. That said, it is worth the effort to try to pinpoint early-warning indicators that signal whether a potential risk effect is turning into reality. Some risk signals are easier to perceive than others. For example, in the case of legislation, the trigger for the risk might be passage of a bill. In contrast, risks related to cloud computing may have several indicators, such as the extent of data migration to third parties and increasing levels of cloud spend. If indicators exist, they should be leveraged to plan for the potential risk effect.

Regardless whether an emerging risk becomes a known risk through the presence of objective indicators or subjective determination, once it happens, the organization needs to prepare. The responsible risk owner can develop metrics and action plans, just as he or she does for other known risks. Sometimes, emerging risks and known risks converge. For example, consider the impact of an emerging risk such as changing labor laws overseas on outsourced operations. This emerging risk has the potential for disrupting the already known risks of market pricing and currency fluctuations. The combination may exacerbate volatility and/or create new vulnerabilities that also need to be considered. In such circumstances, it may be difficult to pinpoint a single risk owner. Instead, a cross-disciplinary response may be required.

Overcoming Challenges

Developing an emerging risk capability can be challenging in and of itself. As such, it is important to adopt a "test and learn" philosophy at the onset. The risk management function should prepare leadership for the likelihood of new discoveries and course corrections along the way. Key challenges include:

The ostrich in the sand effect

Some emerging risks are perceived as so unlikely to occur that they are unworthy of consideration. To overcome this perception, it is helpful to cite instances of the risk impacting other organizations. No organization can be prepared for every conceivable emerging risk, especially as the rate of complexity continues to grow. The goal is to ensure that the company has focused its attention on high-impact, low-likelihood events, and strengthened its ability to respond generally in the face of such events.

Knowing when to escalate

For emerging risks that lack early-warning signs, it is difficult to know when to sound the alarm. Do it too soon and you are "crying wolf." Do it too late and you have lost your window to intervene. A good gut check is the following question: Can this risk be adequately addressed by those in the know, or does it require senior level intervention to approve some course of action? If the former, then perhaps you want to highlight the risk, but not escalate it. This may seem like a subtle distinction, but in these kinds of conversations, tone matters. Offering senior leadership assurance that you have identified a risk, are addressing it and will keep them apprised, is likely to prompt a much different reaction than asking them to intervene during a developing crisis.

Lack of collaboration

Increasingly, emerging risk issues require interdisciplinary response. For example, it is all but impossible to identify a single risk owner for cloud computing when, to varying degrees, the use of cloud computing may impact nearly every business unit in the organization. It is still important to empower a single leader, but that leader should be held accountable for developing a cross-functional team to respond to the issue. A key criterion for selecting the risk owner should be his or her ability to influence in the absence of direct authority and make sure that every voice is heard.

Knowing the unknown

It is often hard to imagine scenarios apart from the organization's day-to-day existence. To complement the views of internal subject matter experts, external sources, such as Gartner's quarterly *Emerging Risks Report*, the World Economic Forum's *Global Risk Report* and the *Excellence in Risk Management Survey* from RIMS and Marsh should be consulted to round out the list of potential trends.

Conclusion

Although they are often unique, emerging risks can be identified, evaluated and monitored, and response plans can be implemented when they occur. Emerging risk identification and assessment creates a competitive advantage, helps "future-proof" longer-term strategies, minimizes unwanted surprises, and allows organizations to capitalize on opportunities. Understanding the potential impact assists in risk management strategies and may reveal opportunities for new revenue streams. Identifying and evaluating emerging risks empowers organizations to be forward-thinking, leading to increased readiness and resilience in the face of new and developing threats.