What are they saying? New ways to detect emerging reputation (and other strategic) risks

Henry Ristuccia
Global Governance, Regulatory & Risk Leader
Deloitte Touche Tohmatsu Limited

Peter Dent
Global Crisis Management Leader
Deloitte Touche Tohmatsu Limited

Reputation risk often tops the list of those that keep senior executives and board members up at night. That concern is not misplaced. Reputation risk emanates from financial, operating, security, compliance, legal, and other risk events, and when those events come to light, that light can be harsh.

This is particularly the case in the social media and virtual worlds, where incidents and decisions that would escape notice or comment a mere five years ago, now find a global audience ready to take organizations to task within hours and often with serious repercussions.

Not incidentally, reputation risk usually falls outside traditional risk management frameworks and Enterprise Risk Management (ERM) capabilities. Yet reputation risk must be proactively managed as a risk given its ability to damage brands, lines of business, and entire organizations. Indeed, this elevates reputation risk to the level of strategic risks, which means it warrants senior executive and board-level attention.

As with most risks, the sooner reputation risk is recognized and addressed, the better. Yet approaches to managing reputation risk tend to focus mainly on cultivating a good reputation and countering setbacks through effective communication. While essential, these activities are no longer enough, given that reputation risk can emerge so quickly and from so many directions. Management therefore needs explicit means of recognizing the potential reputational impact of an incident or decision and of proactively addressing reputation risk.

The right capabilities, enabled by innovative technologies, can position the organization to identify, detect, track, mitigate, and manage reputation risk—and other strategic risks—more proactively than traditional capabilities and reactive communication. Indeed, many companies are seeking better methods of addressing reputation risk, and working to apply them.

[1] *2014 global survey on reputation risk: Reputation@Risk, October 2014, Deloitte <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf>*

Reputation risk = Strategic risk

Reputation risk is unique in that almost any other risk can—when significant enough—generate reputation risk. Social media and the virtual world have lowered the threshold of significance such that minor incidents or seemingly innocuous decisions (or statements) can damage reputation, unless they are handled well. In addition to financial, operating, security, compliance, and legal risks, risks related to conduct, ethics, and integrity, corporate responsibility and sustainability, and products, services, and customer sentiment can drive reputation risk. Any of these risks within a third-party relationship can also expose an organization to reputation risk.

Reputation risk is a strategic risk in that it can undermine the organization's ability to implement strategies or achieve strategic goals. That is why reputation risk topped the list of strategic risks cited by respondents in the 2014 Reputation@Risk survey[1], conducted by Forbes Insights on behalf of Deloitte Touche Tohmatsu Limited (DTTL).

> Reputation risk is unique in that almost any other risk can—when significant enough—generate reputation risk

That survey of more than 300 executives from companies in every major industry and geographic region found that companies are investing in capabilities for managing reputation risk. More than half (57 percent) plan to invest in related data, analytical, and brand-tracking tools, including media/negative-mention monitoring, social media monitoring, and surveys. Yet respondents in that survey cited the key drivers of reputation risk as relating to ethics and integrity, including fraud, bribery, and corruption (55 percent), followed by physical and cyber security risks (45 percent), and product and service risks (43 percent).

These top three drivers—ethics and integrity, physical and cyber security, and product and service risks—matched those identified by companies that had actually experienced a major reputation risk event. Furthermore, respondents expected these drivers to top the list for at least the next three years. Third-party relationships are another key risk area, as companies are increasingly being held accountable for the suppliers' and vendors' actions. These findings may indicate that organizations should cast a broader net when monitoring reputation risk.

A strategic risk-sensing program provides that broader net. It also provides decision-makers with real-time awareness of events that are likely to affect reputation. Such a program extends beyond news media, social media, and customer sentiment monitoring to identify a wide range of emerging risks early enough for management to head them off or mitigate them. Most leading organizations have some sort of program designed to detect and track emerging risks. However, the purpose, shape, and implementation of these programs vary widely.

[1] *2014 global survey on reputation risk: Reputation@Risk, October 2014, Deloitte <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf>*

Defining risk sensing

On the basis of ongoing work, Deloitte has developed a definition of risk sensing, as well as related concepts, practices, and capabilities. In general, risk sensing uses advanced technologies to selectively scan and analyze the internet and social media for structured and unstructured facts, figures, reports, and opinions for specific emerging risks, risk indicators, and potential risk events. The goal is to detect and track nascent risk events and anomalous data in order to monitor changes, trends, and patterns, and to distill the results into actionable information.

Strategic risk sensing aims to identify, analyze, and monitor emerging risks that could impact reputation as well as other strategic risks to the organization. Advanced analytics, combined with selected risk indicators, enable analysis of data against benchmarks and across potential scenarios with the aim of identifying risks most relevant to the organization's senior executives and decision-makers. Sophisticated scanning and analysis also identifies emerging trends outside the defined risk universe that could eventually impact reputation.

A robust risk-sensing capability encompasses the following characteristics:

Strategic focus

Most major organizations monitor financial, operational, compliance, and other risks to the business. Additional risk-sensing opportunities arise from identifying strategic risks—those that could undermine achievement of strategic goals, negate management's assumptions, or exceed the organization's risk appetite.

Senior executive engagement

Senior executives should ensure that risk sensing remains relevant and is integrated into the risk governance and risk management program. Their involvement should also preclude siloed approaches to risk sensing.

Outside-in points of view

External analysts who understand the organization's goals and risks can often provide more forward-looking, objective views than internal parties. Their views can also correct for the internal biases of management and staff analysts.

Listening posts

Listening posts enable tracking of trends in social media and news sources, such as changes in customer sentiment. Listening posts can also be established to monitor changes in employee sentiment, regulatory expectations, and other specific patterns and trends.

Metrics and tracking

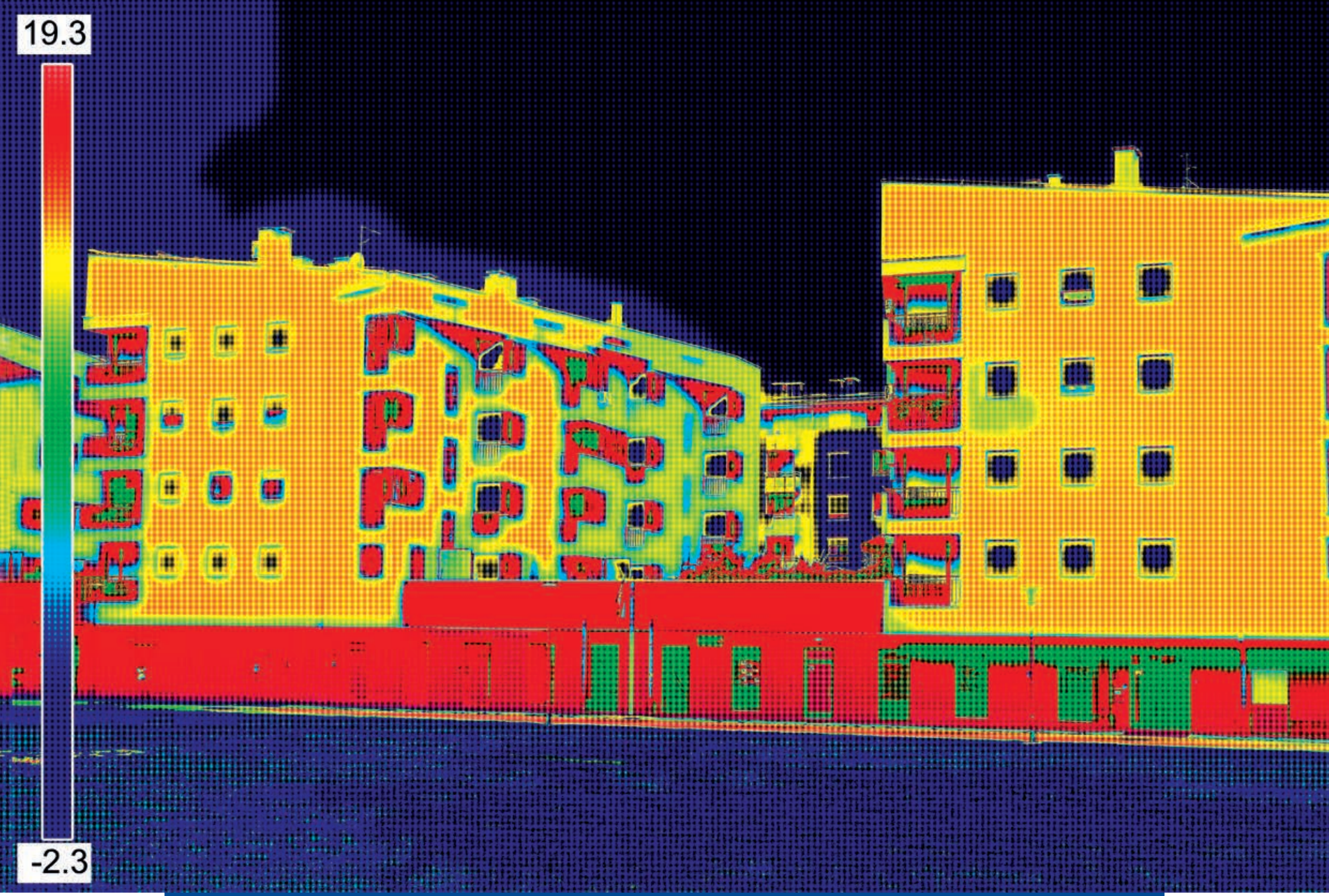
Real-time risk indicators enable monitoring of risks against objective baseline measures and thresholds. A risk-sensing program should also include early warnings and triggers (relative to risk tolerances) for evaluating, communicating, and mitigating risks.

Combined technological and human resources

Analyzing and predicting rare and nascent events has become increasingly possible with advances in text and data analytics. Yet human analysis enriches these views and provides valuable, otherwise unavailable insights.

Rather than reams of data, decision-makers need summary reports, concise insights, and visualization tools such as dashboards. Risk sensing should not be the domain of isolated specialists or technologists. A direct line from the sensing team and the CRO to the CEO and board would be useful, particularly for communicating emerging strategic risks.

Variations among companies' risk-sensing efforts are to be expected, given that risk sensing is relatively new and organizations must adapt it to their needs. Specialized efforts, such as those for detecting changes in customer sentiment, political risk, credit risk, or compliance risk, remain useful. Yet the range of today's risks argues for broad, deep, truly strategic risk-sensing programs. Although the technology and expertise is available, such programs depend on innovative but rigorous application of those resources.



An application of risk sensing

Deloitte uses 24/7 monitoring itself to integrate certain monitoring capabilities into an intelligence platform for filtering and correlating data from social media, news feeds, financial reports, and government agency announcements—among other sources. These capabilities can also be used to monitor post-event impacts, such as effects of a weather-related event on the supply chain of key clients or the reputational impact of cyber incidents.

The 24/7 monitoring methodology addresses risks in five areas: cyber, communications, geopolitical events and man-made or natural disasters, financial crime, and distressed entities. For example, the methodology can be applied in the following areas and ways:

- **Cyber:** malware and data monitoring, cyber watch analysis, confidential and personal data monitoring, targeted vulnerability monitoring
- **Communications:** social and traditional media monitoring, reputation and brand monitoring, privacy and public relations monitoring, industry and competitive intelligence
- **Geopolitical/disasters:** business risk analysis, risks to human resources and infrastructure, real-time disaster and supply chain risk analysis, post-incident resilience and crisis management

Depending on the nature of the threat, this capability can integrate internal data generated by the organization with data from external sources. Automated monitoring detects events, trends, and anomalous data more efficiently and effectively than human analysts; however, human analysts apply experience and judgment to understand the organizational implications of the output.

This capability transforms data into actionable information delivered via an interactive customized dashboard. The dashboard provides both text and graphic incident reports in summary form by category of threat, and monitors the severity and status of the threat.

24/7 monitoring is just one of many forms risk sensing may take. Regardless of the specific form, success depends on the ability of internal and external team members to identify risks to the organization, indicators of those risks, and sources of relevant data—and then to design and implement a platform to monitor all three, and to act on the output.

A look at risk-sensing practices

A DTTL/Forbes Insight risk-sensing survey held in May/June 2015[2] indicates that most large organizations are engaged in risk sensing as they define it. The survey findings—and Deloitte's experience in the field—indicate that risk-sensing efforts are subject to different definitions and are often missing elements that could benefit the organization.

For example, a program may focus on a narrow set of risks, reside in an isolated technical or business unit, or omit other characteristics of a strategic risk-sensing program. As would be expected, organizations also vary in the risks they monitor, the positions to which risk sensing efforts report, and the risks they view as important.

The following are among the key findings of the DTTL/Forbes Insight risk sensing survey:

Companies apply risk sensing, but less often to strategic risks

About 80 percent of respondents agree that they use risk sensing tools. However, based on the top three "Agree" answers on a scale of 1 to 10, they apply them most often to financial risk (71 percent), compliance risk (66 percent), and operational risk (65 percent), and less often to strategic risk (57 percent). Yet strategic risks tend to be most important to senior executives and the board.

Management's perceptions of risks shift slowly

A similar DTTL/Forbes Insights survey carried out in 2013[3] asked respondents to choose the major strategic risks they faced three years prior, at the time of the survey, and three years ahead, as did our 2015 survey. The more recent survey shows that perceptions of risks have shifted somewhat.

- Reputation risk remains among the top three in all three timeframes in the 2013 and 2015 surveys, while economic trends diminish as a concern in 2015. In the 2015 survey, regulatory risk joins reputation risk as a concern in all three timeframes. The pace of innovation stands among the top three risks in 2015 and (in a tie with regulatory risk) tops the list in 2018. These findings indicate that management's views of risks shift, though not quickly. It is therefore useful to define risks broadly, because management's definitions of risk tend to direct risk-sensing efforts. Also, risks rarely remain static, which underscores the need for external viewpoints to provide broader perspective and greater objectivity.

External points of view may be undervalued

Many respondents agree that outside parties have more objectivity about risks than insiders, but even more do not agree. A total of 40 percent "Agree" (as measured by the top three levels of agreement), yet those in the middle range (4 through 7 on a ten point scale) total 51 percent, indicating uncertainty about the value of external viewpoints. This finding may be skewed by respondents who consider external views as including—or consisting of—social media or reviews and ratings on websites, which they may devalue.

- Meanwhile, 10 percent disagree or disagree completely that an outside perspective can analyze risks with greater objectivity. This could indicate strong, potentially dangerous internal biases. External points of view can be particularly useful for weighing risks regarding reputation and the pace of innovation. Organizations can underestimate risks to reputation by overweighting positive customer survey results and dismissing negative views. On innovation, major companies often see new technologies as immature or irrelevant only to find themselves battling new competitors with disruptive business models sooner than they ever thought possible.

A Deloitte/Forbes Insight risk-sensing survey held in May/June 2015[2] indicates that most large organizations are engaged in risk sensing as they define it

Two-thirds believe they have the right people

Two-thirds of respondents agree (based on the top three "Agree" responses) that they employ people with the knowledge needed to monitor, analyze, and act on risk-sensing data. One-third are less certain. The largest companies in the survey—those with at least US$5 billion in annual revenue (as opposed to those in the US$1 billion to US$5 billion range)—most often agree, as may be expected given their deeper talent pool.

- When the risk-sensing team is large, respondents' answers could indicate that the company relies more on people than on technology. While some companies use visualization tools and dashboards, fewer use pattern analysis, scenario analysis, or other leading-edge analytics. The right tools reduce initial data gathering and analysis and free human resources for higher value-added activities.

Risks of most concern in 2013

2010	2013	2016
41% Brand	40% Reputation	29% Economic trends
28% Economic trends	32% Business model	26% Business model
26% Reputation	27% Economic trends/ Competition (tie)	24% Reputation/ Competition (tie)

Risks of most concern in 2015

2012	2015	2018
44% Brand	35% Regulatory	30% Pace of innovation/ Regulatory (tie)
41% Reputation	32% Reputation	25% Talent
32% Regulatory	29% Pace of innovation	24% Reputation

[2] *Exploring Strategic Risk: 300 executives around the world say their view of strategic risk is changing, DTTL, 2013 <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-exploring-strategic-risk.pdf>*

[3] *Exploring Strategic Risk: 300 executives around the world say their view of strategic risk is changing, DTTL, 2013 <http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-exploring-strategic-risk.pdf>*

Getting risk sensing right

Forward-looking organizations are linking strategy development and risk assessment more closely. While many companies have long done this, efforts have often been siloed and thus disconnected. As a result, data on risks and opportunities often goes undetected or fails to make it upstream or to other relevant parties. Meanwhile, data on the next devastating risk or golden opportunity usually already exists within the organization or in cyberspace. Yet no one links that data to the strategic assumption or driver of value that may be (or will be) affected.

A starting point would be for the organization to identify the factors that, if negatively impacted, would alter the forces that drive the organization's sector. Those forces can be organized into domains, such as economic, regulatory, customer, technological, operational, and research and development, and include scientific, engineering, or other advances that could affect drivers of value.

Within specific domains, certain data will reflect existing and potential events and trends related to the sector or organization.

Consider, for example, the following sample issues and themes within each of these common domains:

Economic

Regional and national growth, interest rate and currency environments, sector developments, input costs (including labor), supply and demand dynamics

Regulatory

Legislative developments, regulatory agency priorities, compliance methods and costs, case law and litigation trends

Customer

Product and service preferences, factors influencing purchase, evolving customer journey, competitive product and pricing strategies, technology adoption curve

Technology

Basic science and R&D trends, knowledge transfer, technology commercialization, academic activity, patent filings and citations, technology acquisitions

Operational

Supply chain, alternate suppliers, capacity issues, production and delivery challenges, outsourcing, use of alliances and channel partners

These are sample domains and issues. Actual domains and issues would be specific to the organization and its sector. Also, domains overlap in ways that must be identified so interactions among them can be mapped to risks and opportunities.

Four steps to implementation

Developing, launching, and maintaining a risk sensing program requires dedicated resources, starting with internal people who understand the company's business and unique risks. External resources may also be required, given the need for a technology platform, sophisticated analytics, and outside-in perspectives. Risk sensing also requires the expertise of data scientists, data engineers, and sector analysts to identify required data and data sources, define optimal workflows, and develop formats for dashboards and reports.
Here are four steps to consider when framing and implementing a strategic risk scanning, sensing, and tracking program:

1 Identify the strategic risks to be monitored, and the scope of the effort

Senior leaders and key stakeholders can begin by identifying and prioritizing strategic risks, and agreeing on the risks, domains, and potential disruptors to be monitored. The scope of the effort will be determined by the risks to be monitored, the metrics to be tracked, and the thresholds that will trigger communication, escalation, and countermeasures. Management should define the scope as strategic and enterprise-wide.

2 Define the elements required to enable strategic risk monitoring

The team can then identify the technology and human resources required for the program, which will depend on the risks and data sources to be monitored and desired data extracts and reports. The team must identify the outputs—the data, analyses, flags, and insights—and the visualization tools best suited to representing them. This step should also define the workflows required to analyze the risks, generate the output, and communicate and act upon the results.

3 Configure the platform to enable scanning, sensing, and tracking of risks

After the workflows are structured and the supporting technology and human resources are in place, scanning, monitoring, data extraction, and analysis begin. Initial output is reviewed and early insights are developed. The data and findings can be enriched with sector, economic, marketplace, regulatory, and other information, and the initial results fine-tuned.

4 Continue monitoring the data sources and generating ongoing insights

The team, working with senior executives, risk managers, and other stakeholders, continues to develop insights regarding strategic risks and issues. Users of the output must incorporate the insights into key plans and decisions such as those related to product development and discontinuation, market initiatives, IT purchases, human resource allocation, and mergers and acquisitions. If this is not happening, everyone must learn why—and decide how to make it happen.

The team must continue to sharpen the scanning and analysis, expand or narrow the program's scope, improve dashboards and reports, and deepen the information and insights. Perhaps with external assistance, the team should periodically review and validate the program, considering its scope, practices, resources, and output and then revise elements accordingly.

In terms of the team, in addition to senior executives, business unit leaders, and risk managers, the following individuals would be useful in developing and refining a risk-sensing program:

Specialists

Individuals with expertise in analytic methods, such as developers of process modules

Platform sector analysts

Analysts working with specialists to develop the sector analysis and to define required workflows

Dedicated analysts

Analysts who use the platform, with guidance from sector analysts and specialists, to refine specific reports and reporting mechanisms

The combined technological and human resources give risk sensing its detection and analytical powers. The tools and the people are critical to success.

A risk management essential

These days, seemingly insignificant issues can become global headlines that undermine hard-won reputations. Leading organizations already treat reputation risk as a strategic issue, a trend that should accelerate. Unfortunately, many companies are underprepared to manage reputation risk.

Risk sensing can help in detecting emerging issues, but the right capabilities must be in place before a crisis hits. A true strategic risk-sensing program goes beyond tracking a handful of risks and specific risk indicators in several media. Rather, it identifies a broad range of reputational, strategic, and other risks to the organization, scans myriad sources of data and information, and leverages technological and human resources optimally. It also produces output of high value to senior-level decision-makers.

Recent DTTL/Forbes Insight surveys indicate that most large organizations have risk-sensing efforts underway, but that many may have a way to go if those efforts are to become true risk-sensing programs. In general, the value of an organization's program will reflect the extent to which it is tied to strategic risks and priorities, supported by senior executives, integrated with risk governance and risk management, and comprised of the right resources.

Not incidentally, Deloitte has embedded risk-sensing technology in its own risk governance structure to promote understanding of how brand-impacting events might affect the organization, and to enable adjustments to strategies.

Printed with permission by Deloitte Touche Tohmatsu Limited