TOWERS WATSON

2013 Risk and Finance Manager Survey

Full Report

Executive Summary

The Towers Watson Risk and Finance Manager Survey examines how North American companies use outside resources, tools and frameworks to address risk. Key findings in this year's survey include:

- Two-thirds of survey participants have an enterprise risk management (ERM) process in place.
- Risk appetite and risk assessment metrics and strategies are largely corporate-level decisions that are often not well communicated at the operational level.
- More organizations are starting to purchase a network security/privacy liability policy — the proportion of participants increased 11 percentage points, to 39%.
- In spite of deficiencies in preparedness highlighted by Superstorm Sandy, most participants believe they are sufficiently prepared to handle a major natural catastrophe.
- Only 10% of survey respondents that have a captive use it to fund any employee benefit coverage.

Participant responses suggest a certain confidence that they are increasingly prepared for a variety of eventualities ranging from a hardening market to natural catastrophes and the threat of terrorism. But their responses also reflect a need to build on risk management steps already implemented, as well as the need to regularly review programs to see whether there are additional actions that can be initiated. There is also a need to better communicate risk management strategies so that all stakeholders within the organization are engaged.

Market Snapshots

The Hardening P&C Market

Concern over a hardening market for property & casualty (P&C) insurance coverage is temperate, with 88% of participants citing either moderate or slight concern over the impact such a shift would have on the cost of their risk financing program. The 96% that expressed any concern ranging from serious to slight was roughly unchanged from the 95% response rate last year.

To manage the effects of the changing property market, companies are relying, for the most part, on their ability to market their programs to property insurers (61%, down from 69% in 2012), to implement broker-provided catastrophe modeling (35%) and on the use of captives (24%). But they are also looking beyond these techniques and considering other options as well: evaluating retention levels, pursuing multiyear rate guarantees and self-insuring, to name just a few. For casualty coverage, respondents also ranked marketing of their programs as a number one preparedness strategy (60%, down from 63% in 2012), in addition to relying on independent actuary-provided retained loss analytics (37%), predictive modeling (27%) and captives (24%).

The Benefit Market

While the use of captives is considered a viable risk financing solution for P&C insurance, it has not yet matured into a common means for funding employee benefit coverage, according to 90% of the respondents to our survey. But our survey suggests that this will be changing, as 23% of participants not currently doing so are open to using captives to fund benefits during the next three years. For the 10% of participants that do use captives for benefit funding, the majority fund life insurance, and short- or long-term disability protection, each with a 58% response rate.

The Current Risk Environment

Cyber-Risk

Highly publicized breaches in security and privacy are forcing companies to reconsider how their data and proprietary business information are protected. This new awareness is reflected by the 39% of our survey participants that purchased a network security/privacy liability policy, a sizable 11-percentage-point increase over 2012. The mean value of limits purchased was $18.1 million, up from $12.4 million in 2012. Financial services companies, including insurers, were more likely to purchase these policies (56%) than nonfinancial services firms (33%), possibly because of the amount and importance of personal data required for customer accounts *(Figure 1).* But nonfinancial companies may also be at substantial risk of having data compromised and experiencing severe business setbacks as a result of such a breach.

That growing awareness of exposure was evident when participants that did not purchase a liability policy were asked why. Thirteen percent responded that they did not believe they have a significant data exposure, a 12-percentage-point decline over 2012. Similarly, there was a decline of 10 percentage points from 2012 for those respondents that maintained that their internal IT department/controls are adequate (31%). This gradual shift may speak to the growing awareness that the increasingly sophisticated cyber-attack capabilities of hackers could require a more comprehensive protective net than a reliance on even the most capable IT staff *(Figure 2).*

Among respondents, financial services companies that didn't have a liability policy in place were more likely than nonfinancial services respondents to cite the adequacy of their internal IT departments/controls (36% versus 29%) or the prohibitive cost of a risk transfer solution (22% versus 10%). Perhaps the day-to-day demands of protecting sensitive consumer information and the regulatory penalties for failure to do so have prompted financial services providers to fortify IT functions. But the results are still somewhat surprising, because one would assume that financial services participants would have more efficient risk transfer solutions at their disposal than nonfinancial services respondents.

Figure 1. Companies that have purchased a network security/privacy liability policy

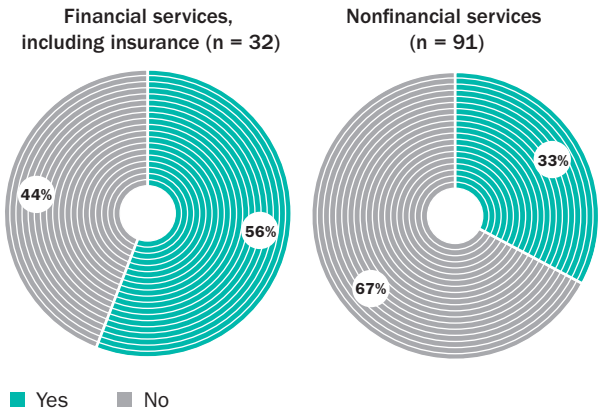
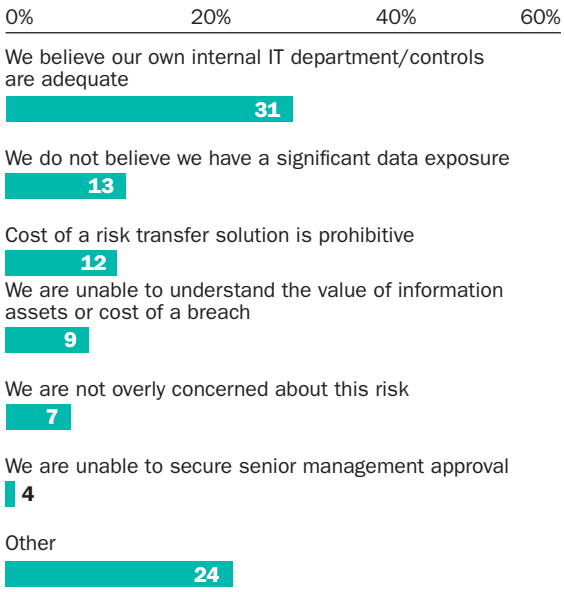


Figure 2. Reason for not having a network security/privacy policy



Base: Companies not purchasing a network security/privacy liability policy (n = 75)

"Highly publicized breaches in security and privacy are forcing companies to reconsider how their data and proprietary business information are protected."

Still, the sizable number of companies that do not have a liability policy in place speaks to the need for more education and a better understanding of the long-lasting financial and reputational costs that companies face if they don't develop comprehensive risk strategies to thwart cyber-attacks. These strategies also need to be flexible enough to adapt as these attacks evolve. Benchmarking information and broker recommendations may be fertile educational sources. In fact, 61% of respondents that purchased liability coverage used benchmarking information, and 47% relied on broker advice when selecting a limit level for their network security/privacy liability policies. Benchmarking information could be updated as the nature of cyber-risks changes, and brokers would offer an efficient way to communicate new market responses to these attacks.

The rationale for a policy purchase needs to be part of that education. By far, most participants selected an insurer based upon its expertise in breach preparation and response. Fifty-eight percent ranked it the number one consideration, compared with a 45% response rate in 2012. But there was also an increased scrutiny of pricing: 17% ranked it a number one consideration, up from 9% in 2012. Although it is always a sound business practice to watch costs, it is important to define cost more broadly to reflect the reputational loss that would occur if the response to a cyber-attack were not well executed.

Travel and Terrorism Risks

Travel Risks

Participants indicated that they are managing travel risks largely by travel itinerary tracking (55%), a reliance on their relationship with an external crisis management or security company (45%), or a trip risk assessment produced by an external vendor (40%). Nonfinancial services firms were far more likely to depend on their relationship with an external crisis management or security company, with a 51% response, compared with a 27% response from financial services participants. These responses suggest that the benefits of these activities are well understood. But with only 19% of respondents providing pre-deployment training for high-risk travelers, travel risk vendors may need to do more to deliver simple and cost-effective solutions for traveler preparation. For instance, eLearning programs, which are easy to roll out, could be introduced.

Of real interest is the 29% of respondents that reported that they now see the "duty of care" benefits of physical tracking technology for high-risk travelers. Over the past three years, these solutions have become more cost effective, reliable and robust. Technology will be genuinely useful in travel risk management, and its evolution is likely to be further integrated into this particular area of risk management.

Terrorism Coverage

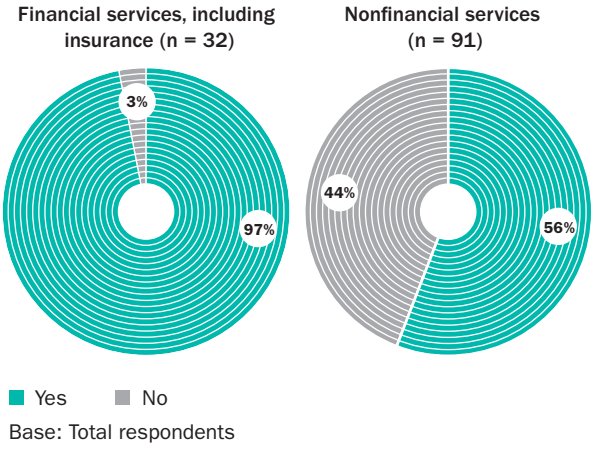
Our survey found that 92% of respondents expressed moderate to no concern over the December 2014 sunset provision in the Terrorism Risk Insurance Program Reauthorization Act (TRIPRA), the successor law to the original legislation, the Terrorism Risk Insurance Act (TRIA). Initially, these findings may seem surprising, but a further review offers another perspective. Sixty-two percent of our survey participants are considering some action to ensure terrorism coverage. The survey allowed respondents to select multiple actions: 32% indicated they were reviewing their coverage to reevaluate their purchasing strategy; 27% were reviewing the rates for TRIA coverage following any change to legislation, and 17% were seeking quotes for stand-alone coverage to compare against TRIA. The very fact that there is this level of uncertainty and alternate planning 18 months prior the law's sunset is concerning, and speaks to the need for Congress to take early action to mitigate potential negative impacts on the terrorism insurance market.

Risk Mitigation Strategies and Actions

Enterprise Risk Management

ERM is being used by 67% of our survey's participants, an increase of 10 percentage points over 2012. However, this number is skewed, as nearly all financial services respondents (97%) employ ERM, which far surpasses the 56% of nonfinancial services respondents that have an ERM process in place *(Figure 3).* Financial services providers must ensure that they are fiscally sound because of their responsibility to account holders and policyholders. Additionally, they face expanded regulatory scrutiny with new requirements from the Dodd-Frank Wall Street Reform and Consumer Protection Act, and for insurers, the Own Risk and Solvency Assessment (ORSA). While nonfinancial companies do not have the same drivers, they would benefit from the lessons learned in the approaches taken by financial services firms with their ERM programs. ERM can help organizations better manage risk, realize operational benefits such as lower borrowing costs, and improve the decision-making process, which can create value for the company.

Figure 3. Companies with an ERM process in place



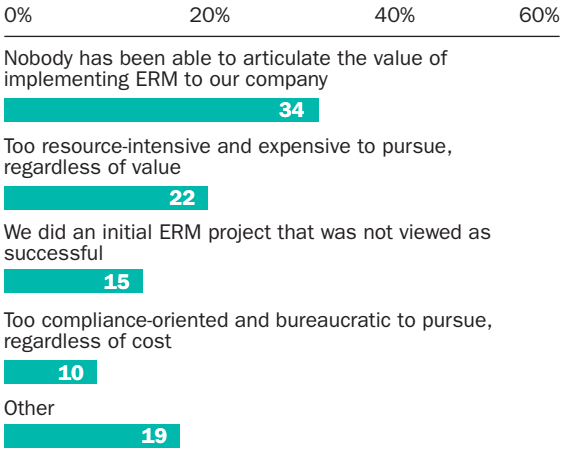
Base: Total respondents

Companies with ERM programs have well-defined processes, but need to better integrate them into their operations and decision-making processes. Well over three-quarters (83%) identify, assess and prioritize key risks and assign owners, and nearly three-quarters (72%) provide the executive committee/board of directors with regular ERM reports. But only 40% regularly quantify key risks and use these metrics in making business decisions, and just 28% of these respondents' executive committees/boards of directors actively use ERM as part of their strategic decision-making process. This disconnect between process and action is again evident in the 24% response rate of those that integrate risk metrics into their budgeting and planning processes. The divide between process and action is even more common among nonfinancial services respondents. And it surfaces yet again when respondents are asked how integrated the risk management function is in strategy and business planning. A scant 3% of all participants indicated it was very integrated; 20% indicated it was integrated, and 43% said it was somewhat integrated. But a third of participants responded that risk management is minimally integrated (23%) or not integrated (11%).

When companies haven't instituted ERM programs, communication and cost were the drivers. Over a third of respondents that did not have ERM noted that no one had articulated the value of ERM implementation for their companies. And 22% expressed just how resource-intensive and expensive it was to pursue, regardless of its value. These results are not surprising given that very few companies use quantitative metrics for risk management *(Figure 4).*

"Companies with ERM programs have well-defined processes, but need to better integrate them into their operations and decision-making processes."

Figure 4. Reason for not having an ERM process in place



Base: Companies not having an ERM process in place (n = 41)

Risk Appetite and Assessment

When risk appetite is determined, it is largely at the corporate level, based on qualitative judgment (33%) or on financial metrics (23%), rather than on the operational or departmental level (8% for both qualitative judgment and financial metrics, respectively). What's even more surprising is that a sizable 22% of participants have not explicitly set any risk appetite level. The results suggest that there needs to be a better understanding of the value of formally establishing a risk appetite, and integrating it seamlessly at both the corporate and operational levels.

Similarly, risk assessment results and strategy are regularly communicated to risk owners and the executive team as part of the business planning process (72%), but less emphasis is placed on the training of employees on general risk issues such as information security, employment practices and workplace safety (43%), or the assignment and training of risk owners (20%). And even when they are communicated to senior management, 57% responded that risk financing alternatives and decisions weren't communicated in financial metrics, even for financial services companies (50%). The ability to communicate using financial metrics could increase understanding and make company decision makers more amenable to risk financing options.

Preparedness

Our survey noted that Superstorm Sandy highlighted deficiencies in preparedness for natural calamities and asked our participants about their companies' general readiness for certain property insurance functions, such as property asset management and the claim process. Overall, the extent of companies' preparedness ranging from "very prepared" to "somewhat prepared" was in the 90% to 94% range.

The one area where there was a noticeable discrepancy was in vendor identification — such as vendors selected for restoration and forensic accountants. Only 77% of respondents cited some degree of preparedness, with a sizable 16% noting some deficiencies, and 7% considering their companies unprepared. This finding is concerning because a company that does not have adjusters and forensic accountants identified prior to major catastrophe losses will have trouble getting its claim process moving quickly. There is a critical distinction between having identified vendors and having already established a relationship with them, and merely having them named in their policies. If they don't have commitments from vendors, they will need to wait in line when a major catastrophe strikes. This time lost could have a critical impact on the long-term well-being of companies.

"In spite of deficiencies in preparedness highlighted by Superstorm Sandy, participants believe that they are prepared to handle a major natural catastrophe."

Taking Stock

The results of this year's survey give us some cause for optimism, but also make us very aware that there is still much work to be done. ERM is used by a full two-thirds of survey participants. While this is a handsome 10-percentage-point increase over last year's results, the growth is from financial companies, showing there is still much to be accomplished with nonfinancial organizations. Companies realize the need to formally recognize and manage risk. Part of this risk management is extending to the evolving risk of a cyber-event, but the 39% purchase rate is still woefully low when the full potential for debilitating corporate damage is assessed.

Only with full company-wide participation will a holistic approach to risk management occur. And yet there are evident lapses in the integration of risk assessment and the communication of risk appetite from the corporate through the operational levels of many respondent organizations.

These gaps are not a cause for alarm, but rather a call to action. It is part of a regular self-assessment process that needs to take place if companies are to ultimately enjoy a comprehensive risk detection and management program that fortifies all their stakeholders.

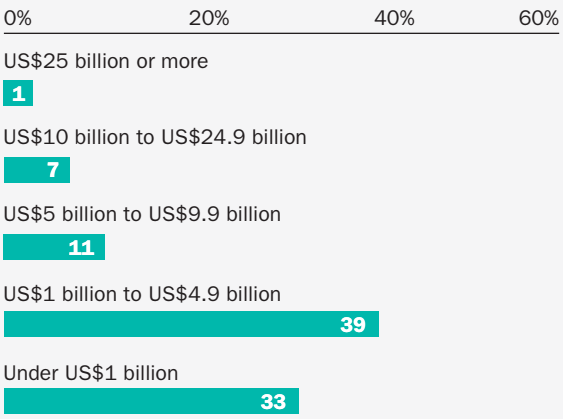
About This Study

Towers Watson's fourth annual Risk and Finance Manager Survey examines how North American companies address risk. The online survey of 123 individuals was conducted from February 26 through March 13, 2013.

Nearly three-quarters of the participants were from companies with total 2012 revenues of under US$5 billion; 39% had revenues from US$1 billion to US$4.9 billion, and 33% were under US$1 billion. One percent of the companies ranked in the largest revenue range of US$25 billion or more. The mean for all participants was US$5.6 billion *(Figure 5).*

The majority of respondents were from the manufacturing (22%) or insurance (20%) business sectors. Health care participants (excluding pharmaceuticals) represented 9% of the survey population, with the education sector represented at 7%.

Figure 5. Total revenues in 2012



Base: Those giving a valid answer (percentages exclude "prefer not to say") (n = 120)

About Towers Watson

Towers Watson is a leading global professional services company that helps organizations improve performance through effective people, risk and financial management. With 14,000 associates around the world, we offer solutions in the areas of benefits, talent management, rewards, and risk and capital management.

TW-NA-2013-29994