Organizational Dynamics: A Focus for Effective Risk Management

CONTENTS

REPORT ANALYSIS AND REVIEW

BRIAN C. ELOWE
Marsh

CAROL FOX
RIMS

INTRODUCTION

Understanding change is fundamental to the practice of risk management. Successful risk executives must be able to define, plan, forecast, and finance for change — and be able to paint a picture of what it means for their organizations. Risk professionals also work in a time of changing expectations around their own roles.

One of the biggest changes, as noted in the 2014 *Excellence in Risk Management* study, is that risk management has become more involved in providing input to develop business strategy in many organizations. That theme was again borne out in the 2015 survey and in complementary focus group discussions with risk professionals: "There is significantly more interest, buy-in, and enthusiasm from our executives about looking at strategic risk rather than just operational or financial business risk," the head of the enterprise risk management (ERM) division at a large public entity told us.

Yet, at the same time, ERM and similar efforts are being evaluated as to their ability to create a positive impact. The 2015 *Excellence* report looks to understand the organizational characteristics that positively affect the execution of a risk management strategy. Successful risk executives strive to ensure that they and their organizations have a clear point of view about risk management priorities, how those priorities may change, and where organizational gaps in alignment exist. To execute on these elements, they need to understand how the decisions regarding risk management investments, structure, communications, and measurement impact their growing strategic role.

Aligning stakeholders in an ever-changing environment can be a challenge. Many current measurement methodologies fail to uncover the value that risk executives bring to their organization. Nonetheless, the critical risk management functions continue to advance and their overall influence grows. Given the complexity of the global business environment, this dynamic is unlikely to slow any time soon.

ORGANIZATIONAL ALIGNMENT

Alignment among key stakeholders is central to the successful execution of any organizational strategy or initiative. How does risk management stack up against some of the key pillars of successful execution? Priority setting, organizational structure, and performance measurement standards each influence the building of a more effective risk culture.

PRIORITY SETTING

Companies are requiring a "risk perspective" as they develop business strategy, and risk management executives are uniquely positioned to provide the bigger picture around risk. In so doing, they can bridge the gaps between their boards' view of risk and the way managers at the operational level see risk. Connecting the two can pay big dividends given the expanding volatility associated with geopolitical, operational, technological, and human capital risks.

How aligned are organizations around some current risk management priorities? For several elements that are fundamental to risk management focus, about two-thirds of our survey respondents said there is agreement at the senior management level (see Figure 1). Notably higher alignment (79%) was found regarding the function's reporting structure, while notably lower alignment (44%) was seen around the use of analytics in risk finance.

We also looked for signs of alignment — or gaps in alignment — related to where organizations said they are investing in risk-related functions (see Figure 2).

CONTINUES ON PAGE 4

"One of the things I would identify as being a large risk is the fact that we aren't aligned as well as we'd like to be."

– Risk executive at a metropolitan port authority.

FIGURE 1 Leadership Alignment

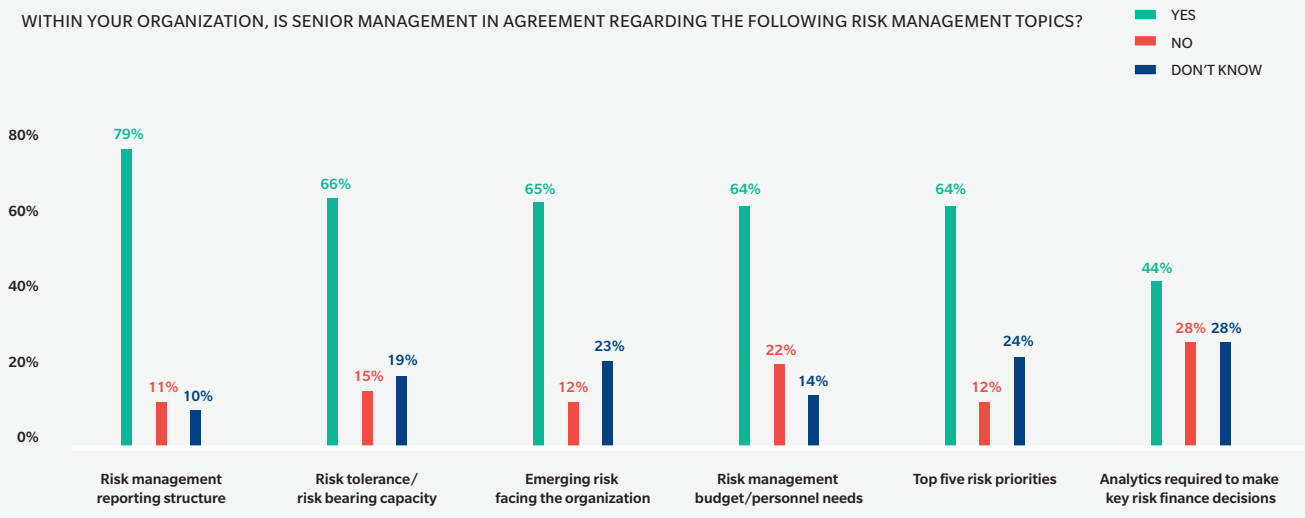


FIGURE 2 Investment in Risk Management

PLEASE INDICATE THE CHANGES, IF ANY, TO THE LEVEL OF INVESTMENT IN THE FOLLOWING OVER THE NEXT TWO YEARS:

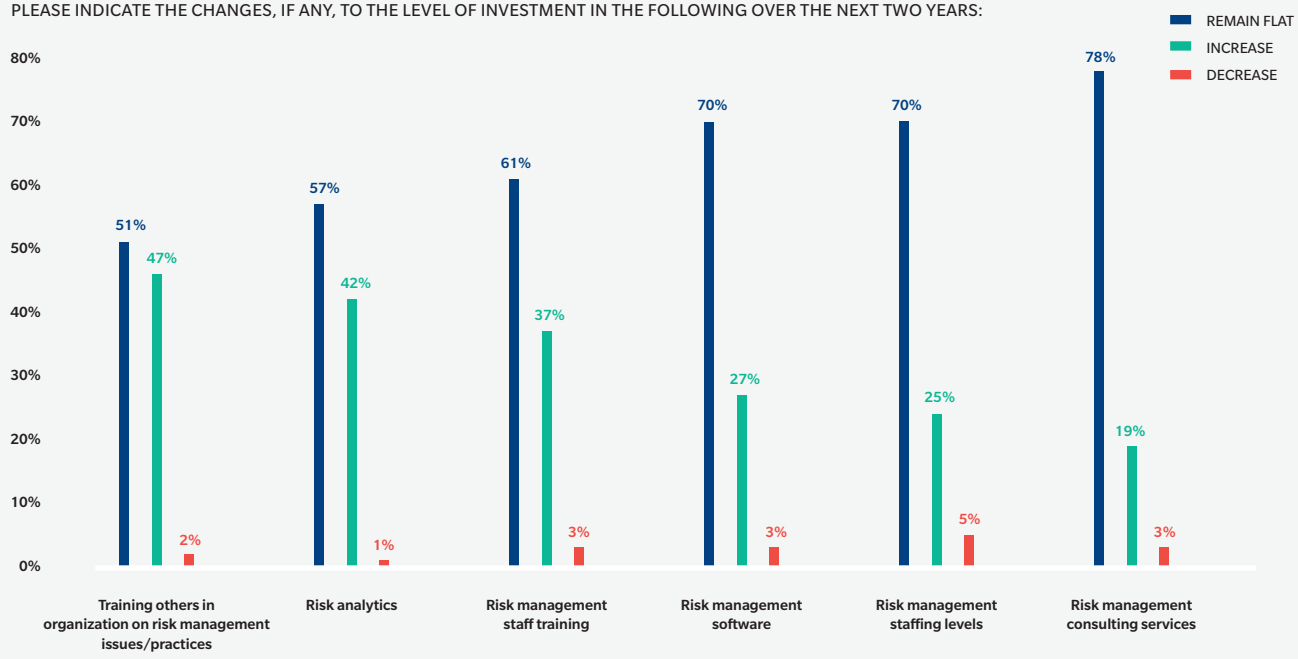
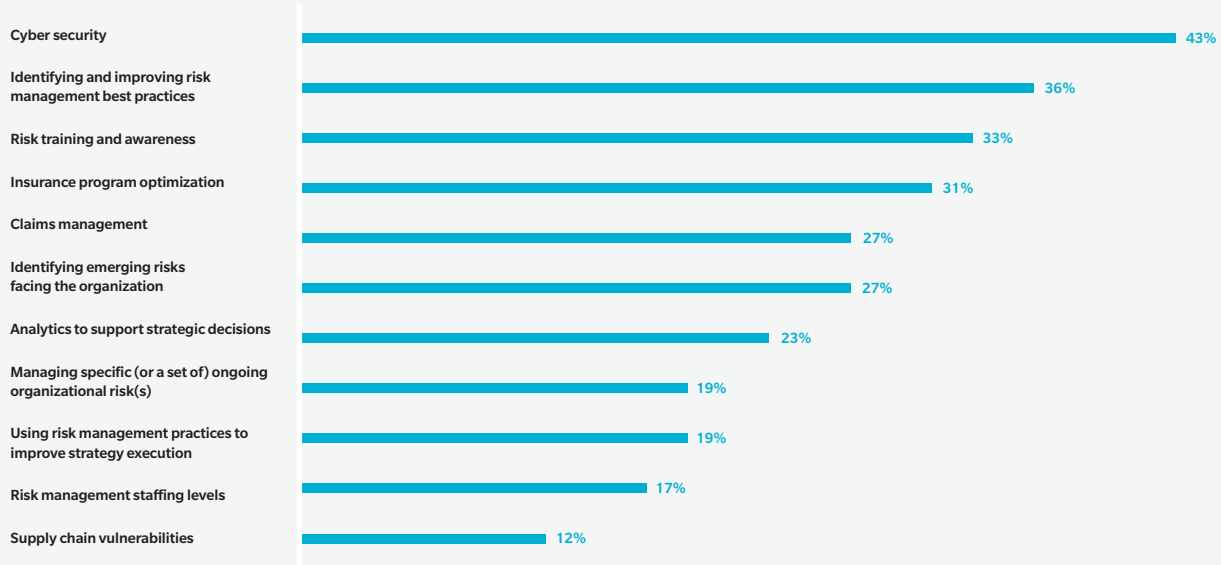


FIGURE 3 Risk Management Priorities

OVER THE NEXT 12 MONTHS, WHICH OF THE FOLLOWING AREAS OF RISK MANAGEMENT WILL BE A PRIORITY(IES) FOR YOUR ORGANIZATION?*



*RESPONDENTS COULD CHOOSE THREE FROM THE LIST.

27% of respondents said that identifying emerging risks would be a priority in 2015.

CONTINUED FROM PAGE 2

Looking at the alignment between planned investments and risk management priorities (see Figure 3), we found most areas to be aligned, with a few exceptions:

- **Not aligned:** Organizations that noted insurance program optimization as a top priority were actually less likely than others to increase investment in analytical capabilities (36% compared to 42%).

- **Aligned:** Organizations that noted risk analytics as a priority were more likely than others to increase investments in:
  - Analytics to support strategic decisions (55% compared to 42%).
  - Risk management software (43% compared to 27%).
  - Staffing (33% compared to 24%).

Focus group participants echoed these results, but were quick to point out that execution of these priorities was often a challenge. They viewed increased alignment at the top of the organization as a positive, but the dominant feeling was that the further removed from leadership, the more likely they were to find disagreements.

A risk executive at a large energy firm gave an example related to its goals of promoting environmental sustainability. "If you talk to some of our operations people compared to some of our sustainability people, there's a very broad divergence about what that actually means and what that looks like," he said. "That creates some challenges in terms of timing and sequencing and prioritization of different activities: Our sustainability folks will want to do one thing to help manage a risk, while the operations folks will want to do something completely different."

EMERGING RISKS

Although we found generally effective alignment on the noted priorities, members of the discussion groups agreed that a focus on the "here and now" is the predominant guiding principle and that more needs to be done to understand emerging risks. They worried that the board view on risk can be overly influenced by regulatory disclosure requirements and compliance, whereas those closer to operations often have a greater understanding of the impact that broader issues have on the bottom line.

Only 27% of risk professionals surveyed said that identifying emerging risks would be a priority in the coming year. This runs counter to the clear message being heard from boards that they are more concerned about "what's around the corner." For example, could geopolitical events introduce volatility into strategic plans? Or what impact might climate change or water scarcity have on operations or expansion decisions?

One of the leading studies to examine such overarching risks is the annual World Economic Forum (WEF) *Global Risks Report*. The 2015 *Excellence* survey asked how companies view the potential impact from some of the top global risks discussed in the WEF report (see Figure 4). The responses indicate that more can be done to elevate discussion of these issues within organizations, with an eye toward potential long-term operational and/or financial impacts.

We also noted the effect that media attention can play. Consider that in 2014, 52% of respondents said that cyber attacks were "already a concern" within their organizations. Likely driven in large measure by the daily drumbeat around cyber events, that number rose to 72% in 2015. Perhaps this indicates that risk executives have been successful in using the broad attention given to cyber risk as a means to engage their organizations in conversation. If so, it's a model they should consider expanding on to prompt conversation on topics such as geopolitical instability and fiscal and water crises.

The ways in which risk professionals seek alignment on emerging risks vary according to an organization's needs, structure, and goals. Nonetheless, questions remain: How are emerging risks identified, be it at the global, industry, or organizational level? Who evaluates

FIGURE 4 Impact of Global Risks

We chose 11 of the risks that the WEF *Global Risks 2015* report listed as top concerns in terms of impact and likelihood. For each one, respondents were asked for the time frame in which they expected it to impact their organization. The top three choices for each time frame were:

IS CURRENTLY A RISK FOR THE ORGANIZATION	WILL BE A RISK WITHIN THREE YEARS	WILL BE A RISK IN MORE THAN THREE YEARS	WILL NEVER BE A RISK FOR THE ORGANIZATION
Cyber	Energy	Water crises	State collapse
Natural catastrophe	Natural catastrophe	State collapse	Climate change
Infectious disease	Fiscal crises	Fiscal crises	Water crises

them, and how? What discussions occur around them? Some of the common best practices among the focus group participants were:

- **Leverage your company's risk committee.** A common refrain: "If you don't have one, get one."
- **Challenge conventional thinking** by sharing reports like the WEF's. Raise awareness and discuss how global risks could manifest in your organization, creating volatility in future years.
- **Reach across the company.** Line managers often have a view of risk that is more grounded in the business. As a risk executive at a technology firm noted: "I can't do much about technological obsolescence, but I can improve many other areas of risk often overlooked by our C-suite."
- **Conduct more scenario planning.** Checklists have their place, but involving operations, finance, human resources, and others in scenario evaluation can lead to actionable insights.
- **Collaborate with internal functions.** Share the benefit of risk metrics with research and development, finance planning and analysis (FP&A), and other departments.

ORGANIZATIONAL AND REPORTING LINE DYNAMICS

Reporting structures, too, can complicate communications with senior leaders.

"We have a huge compliance area — they don't report to us, we don't report to them. We report to finance, they report to legal. And then we have a huge privacy area. And then we have a huge legal area," noted the director of risk management at a major health care company. "You don't know who's got the ear of the board and what kind of information it might be getting that's not necessarily good information, not the information you would've wanted to get there."

The key to managing such problems, she said, is to focus on strategic alignment rather than on functional alignment. "When I think of alignment, I think of partnerships and I tell my staff that we just want to be really good business partners. We're not always going to be in charge."

We asked this year about risk management reporting lines in order to understand how the intersection of those structures and internal alliances impacts the execution of risk management. To begin with, the majority of risk professionals in our survey said that their risk management department reports into the CFO/treasurer (see Figure 5).

FIGURE 5 Organization: Where Risk Management Reports

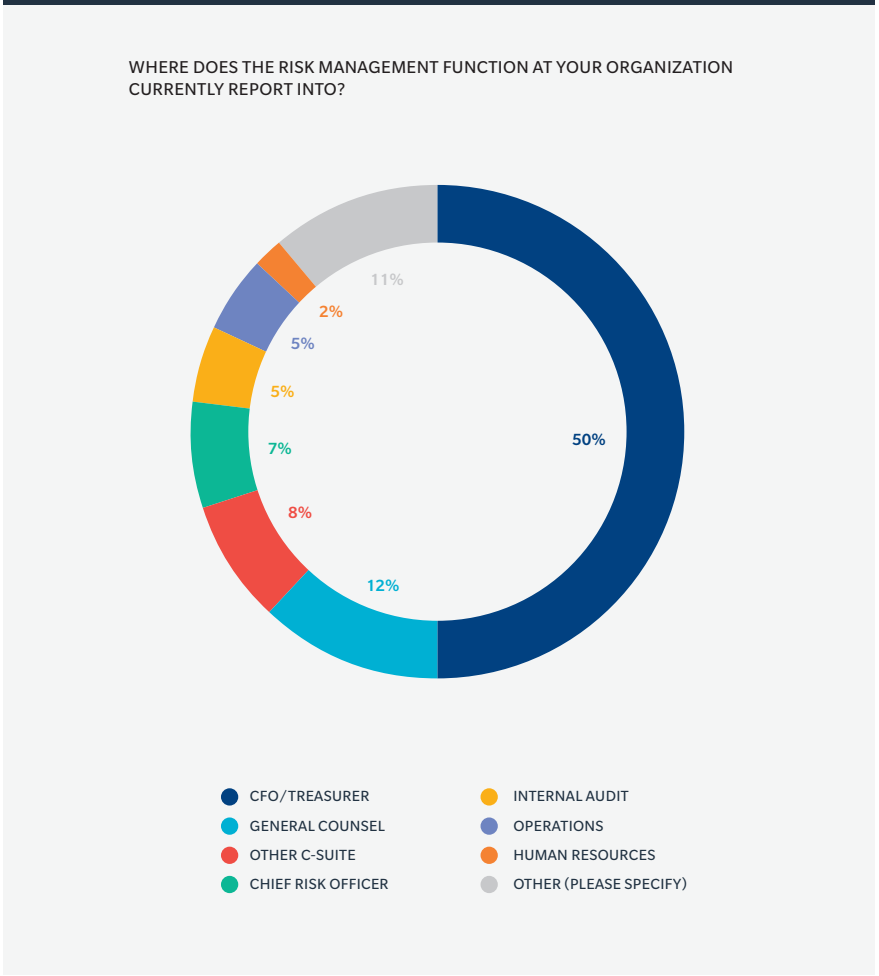


FIGURE 6 Organization: What Reports to Risk Management

We then looked at the other functions that relate to risk management and viewed the responses based on where risk management reported into (see Figure 6).

Although traditional risk management functions like insurance and claims management had no discernable differences based on reporting lines, several perspectives are worth noting. These include:

- Many respondents said that IT risk management (37%) and privacy management (36%) report into the risk function, with another 7% recommending that these areas should report to risk management. This is likely a manifestation of the growing focus on cyber risk. If so, we would expect to see an increase in those percentages in coming years.

- Just under 10% said that business continuity, environmental management, safety, and security should report to risk management on either a direct or "dotted line" basis, while many indicated that these areas already report on a direct or dotted line basis. This reflects a growing alignment and collaboration across other organizational functions that have a relationship to risk management.

- Just over 70% of respondents noted no interaction with their organization's supply chain. This was surprising given the potential for business disruptions such as those that followed the 2011 Japanese tsunami and the ever-growing cyber business interruption risks emanating from suppliers and vendors.

- More than 70% said there was no reporting relationship with internal audit. This may reflect recognition of internal audit's need for independence in providing assurance of the organization's risk management practices. Several focus group participants raised concerns that when ERM functions report to audit it tends to create a "rear-view mirror" as opposed to a prospective approach to risks.

Is risk management properly positioned for greatest effect? Our findings reflected a difference between those risk management departments reporting to the CFO/treasurer and those reporting elsewhere. For example, 27% of those who report into the CFO/treasurer expect an increase in spending for training risk management staff, whereas 46% — nearly double — of those reporting elsewhere expect an increase.

Alignment with other, more strategic functions is generally higher (nearly double in some cases) when risk management reports into somewhere other than finance. This is most notable in the areas of ERM, compliance, IT risk management, privacy, and security. This may be a point worthy of greater consideration by finance executives. Does their primary focus on cost and finance limit the broader organizational value that risk management can provide? Do other functions (for example, legal) have more budgetary flexibility to invest in the forward-thinking resources necessary in today's riskier world? It appears that finance executives will be well-served to facilitate greater organizational connections for their risk management departments in order to position them for broader impact across the enterprise.

Most respondents said they are satisfied with the reporting lines of their departments; and more than three-quarters said that their senior management agrees with the current structure. However, organizations tend to restructure often, whether it's to accommodate mergers and acquisitions, grow globally, respond to changes in strategy or leadership, look for cost savings, or simply to shake things up.

Focus group participants experiencing organizational restructuring that involved risk management departments shared some of their experiences:

- For some, change brings struggle. "We have to work far more strategically to deliver our services with very limited resources," said the risk management director at a health care organization that recently reorganized into a holding company structure. "We're only delivering what they want to see upstairs, so to speak."

- For others, change is an opportunity to grow and reposition. Recent restructuring at a major university system led to the risk management function reporting higher up. "We've got direct input into the president's office when we need it," said the risk executive. He said the increased visibility has allowed significant progress in implementing the institution's enterprise risk management program, which had been stalled under the previous administration.

- Growth in global markets creates pressure in delivering risk management. Risk executives often lead "virtual" risk management functions, working with colleagues who report to their local operations. Cultural interpretations and the lack of direct influence often impede a truly global risk management strategy.

- Some see organizational change as an opportunity to look critically at the risk management function itself: "It forces you to reevaluate what you do, how you do it, and why you do it," said a risk professional who has seen a number of longstanding senior leaders in the company leave in the past year. "When you're telling people what you do, it's hard not to look back and say, 'Are these the best things and the right things we should be doing?'"

Solving Alignment Issues

ORGANIZATION	ALIGNMENT ISSUE	SOLUTION
A metropolitan port authority	Competing priorities among business units.	Working with senior leadership to educate board and find alignment on organizational risk priorities.
Health care company	Integrating strategic risk into the organization's larger strategic business planning process.	Gained a seat on the organization's strategy development committee to help align risk management to business strategy.
School district	Treating risks differently from school to school is hurting the district's bottom line.	Changing the culture at the operational level to align individual schools to overall policies.
Auto manufacturer	Enterprise risk management program iterations not working as desired.	Willing to continuously improve the ERM process to help foster buy-in and alignment.
Financial services provider	Supplier risk management not optimized at operational level.	Moved reporting to chief risk officer to help better align across the organization.

The above examples were provided by participants in our Excellence in Risk Management focus group sessions.

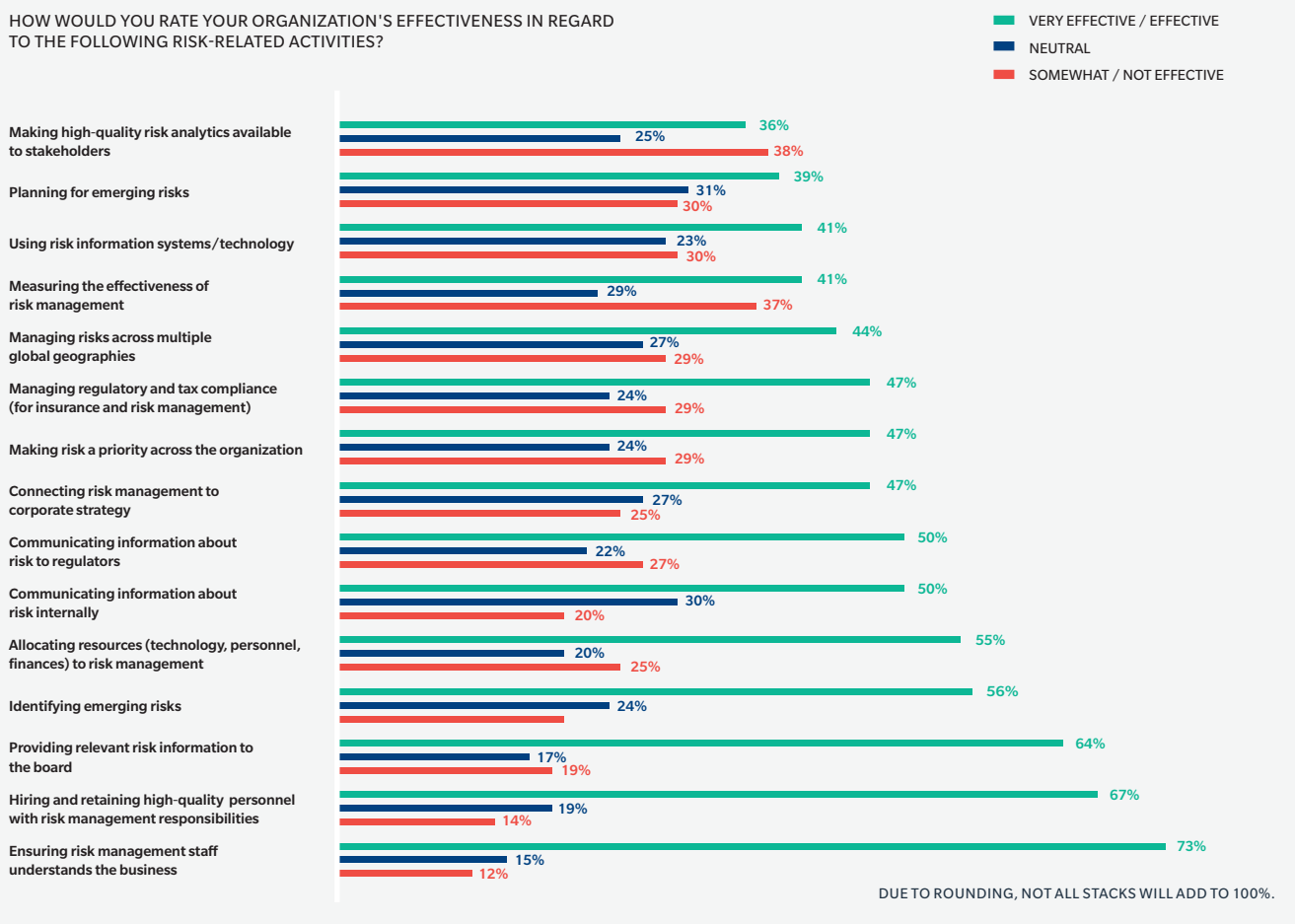
RISK MANAGEMENT EFFECTIVENESS

Finance and human resource executives frequently work with capital allocations, budgets, and employee performance targets to align individual goals and corporate strategies. We looked at how risk management operations employ similar practices as they seek greater focus on improved execution of risk management priorities. We viewed the results through three lenses:

- How effective is the organization in key risk management functions?
- How effective are organizations in collaborating with various organizational functions on key risk management protocols?
- What performance standards are used to measure effectiveness and organizational alignment?

We asked respondents to rate their organization's effectiveness in a number of risk-related functions (see Figure 7). The results indicate that more can be done in the areas of analytics and connecting risk management to strategy; both areas ranked low. Making high-quality risk analytics available to stakeholders not only received low ranks for effectiveness, it also had the highest percentage of respondents saying their organization was "ineffective" (38%). The following are the top functions where respondents said their organizations were "very effective," "neutral," or "not effective."

FIGURE 7 Risk Management Effectiveness



COLLABORATION ON RISK MANAGEMENT PROTOCOLS

Most risk executives understand that the actual management of risk takes place within the day-to-day operation of the enterprise. Thus, deploying best practice risk management protocols across the enterprise is a central requirement. In this year's survey, we asked how involved various parts of the organization* are in four key risk management protocols: risk committee participation, risk management strategy development, risk assessments, and risk response. We found an array of practices, and some gaps:

Risk committees: Representation from business units was noticeably absent from corporate risk committees, although safety and compliance played prominent roles. This supports the premise raised by some focus group participants that — from a corporate alignment standpoint — there is often too much focus on "checking the box" as opposed to discussing areas such as emerging risks. This represents a potentially missed opportunity for operational leaders to add value.

Risk management strategy development: The top five areas identified as being involved in strategy development were executive management, finance/financial planning/treasury, safety management, legal, and business continuity/crisis management. Note that neither the strategy function nor operations were in the top five.

Risk assessments: Operations and information technology were in the top five areas identified as being involved in risk assessment, along with safety management, business continuity/crisis management, and legal. This supported an observation by the head of risk management for a public entity that day-to-day operators and front-line managers are most in tune with the operational risks facing the organization. It also points to the reliance on information network and technology in driving the business engine.

Risk response: From a risk response standpoint, the top five areas cited were business units/operations, safety, business continuity/crisis management, legal and, not surprisingly, public relations/communication. This reflects a post-event "damage control" perspective, rather than an emphasis on developing alternative responses for avoiding or preventing losses or, when feasible, exploiting a risk.

Safety management, business continuity/crisis management, and legal were the functions most widely represented in all four protocols. Absent from involvement in any of the risk management protocols were research and development/innovation. This is especially notable given the high importance of risk management for strategy development, as found in previous years' *Excellence* surveys and echoed by most focus group members.

"My primary role is to drive dialogue around emerging risks."

– Director of risk management at a pharmaceutical firm.

* The functions listed in the survey were: Actuarial; business continuity/crisis management; business units/operations/production; compliance management; environmental risk management; executive management; finance/financial planning/treasury; human resources; internal audit; information technology and network; legal; public relations/communication; quality control/product management; research and development/innovation; safety management; security management; and strategy development.

MEASURING SUCCESS

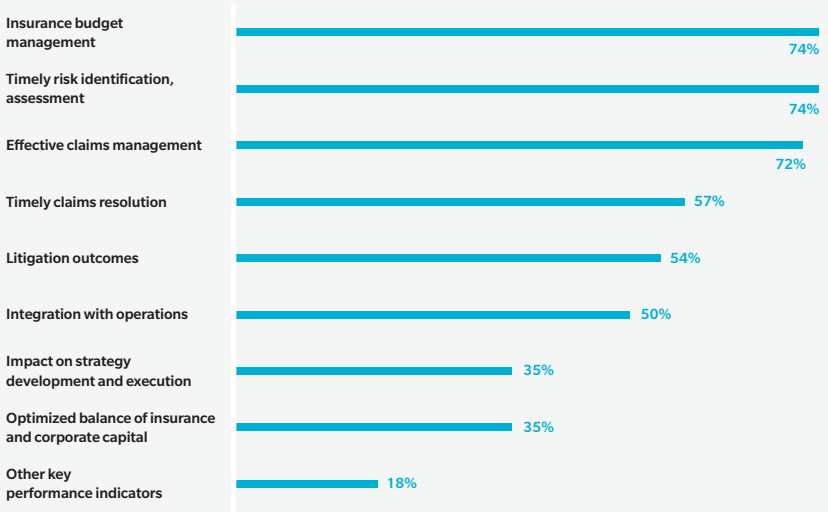
As increased expectations lead risk management to become more involved in business strategy, it is developing into a value-creator as well as a value-preserver role in organizations. With this evolution, it becomes ever-more important to be able to measure risk management's effectiveness, and to do so in ways that reflect the change.

Currently, most risk management departments report being evaluated on traditional measures, such as insurance budgets and claims management results (see Figure 8). The most traditional, insurance-focused risk professionals in our interviews said their departments are evaluated almost solely on budget and peer benchmarking. "The best thing for someone in my position is to be completely out of sight," said the vice president of corporate risk management at a financial services firm. Another said the total cost of risk and litigation — specifically, a lack of — remained the primary measures at his food industry company.

And yet, even those risk professionals who clearly have a more strategic view of their role cited the same types of measures. "The first measurement of risk management performance is: Have we had any really large complex claims, and how have we resolved them or how are we resolving them?" said the vice president for risk management at a global entertainment and media firm. He said a goal is to bring in metrics that "feel more important," such as frequency rate, safety indices, workers' compensation costs, and measures of property scores.

FIGURE 8 Measuring Performance and Effectiveness

WHICH OF THE FOLLOWING DOES YOUR ORGANIZATION USE TO MEASURE THE EFFECTIVENESS OF THE RISK MANAGEMENT FUNCTION*?



*RESPONDENTS COULD CHOOSE AS MANY AS THEY FELT APPLIED.

PERFORMANCE MEASUREMENT FOR VALUE-DRIVEN RISK MANAGEMENT

What is the best way to measure the risk management function's performance based on its strategic value? This became one of the most perplexing questions for participants in the 2015 *Excellence* focus groups. Although there was not a consensus among the group around a single answer, most did agree that shifting to a new performance standard would better reflect the value they bring to their organizations. Based on their responses, the list below represents a starting point for conversations aimed at developing appropriate measurements:

- Achieve earnings (EBITDA) targets, based upon agreed, weighted contribution from risk management.
- Measure outcomes against high priority risks.
- Conduct "customer" satisfaction surveys with business units to evidence how risk management is supporting the business and solving their risk issues.
- Create goals and measure performance based upon self-assessments, leveraging frameworks like the RIMS Risk Maturity Model.
- Measure activity tied to specific goals such as working on the top risks or training needs.
- Incorporate analytical decision frameworks into risk finance strategies and measure outcomes against desired thresholds.
- Measure claim recovery timeliness as a contributor to corporate liquidity.
- Evaluate risk finance structures on volatility reduction in addition to other measures.

Some focus group members noted how difficult it is to find a measure that can be used across the business, especially in a diversified company. "We've been talking with the audit committee to come up with a risk financing optimization model so that they can get a better feel for how our risk financing costs compare to our growth rate," said the director of risk management at a diversified defense company. "We've got a ways to go."

The inability to come up with alternative effectiveness measurements can clearly be a source of frustration for risk professionals. "I wish there were some way we could measure success by thought leadership or by the value we bring to our business partners," said the director of insurance at a leading health firm. "But I can't figure out a metric for that."

Focus group respondents noted some emerging trends worth consideration as organizations look to create dashboards around risk management:

- Move away from budget to a measure of total cost of risk.
- Include qualitative elements, such as feedback from operations that risk management is exporting insights and value to help their businesses thrive.
- Add measures around activities that are known to modify risk effectively.
- Ensure financial allocations include a controllable risk expense.
- Employ analytical methods to compare corporate capital to alternative sources such as insurance and captives as a way to measure efficiency.

DATA, ANALYTICS, AND TECHNOLOGY

Since we first started asking questions about data and analytics in the *Excellence* survey, there has been a consistent call for improving their use. For example:

- In 2011, improving quantification and analysis of risk was among the top three areas where senior management's expectation of risk management had grown.
- In 2013, improving the use of data and analytics was the top answer among risk professionals when asked what their focus areas were for developing risk management capabilities.

But in 2015, fewer than half of respondents (44%) said that senior management was aligned regarding the analytics required to make key risk decisions. That's less than for any other area we asked about, including such areas as reporting structures, risk priorities, emerging risks, budgets, and risk tolerance. This is despite the fact that numerous studies by the Association of Financial Professionals (AFP) and others note the need to employ more analytics in order to create a broader framework for decision making insights.

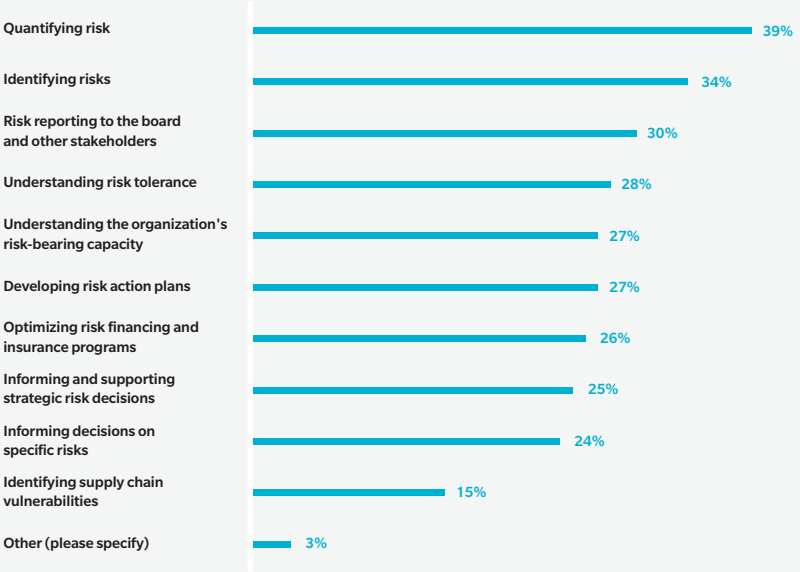
Focus group members offered several lines of reasoning for the lack of agreement:

- The inability of the risk management function to bring together relevant data and provide a coherent, consistent message to leaders. "It confuses some of our executives when they get basically the same metric reported a slightly different way by four different groups with four different numbers," said the risk management lead at a global energy firm. "They say: 'Well, which one is it?'"
- Underlying that can be a lack of planning and training. "We build some pretty neat tools and some pretty good algorithms, and either they don't get used or they sit on the shelf or they're not used in the right way," said the senior director of risk management at a technology services company. This can make it more difficult to present a unified analytics front to senior leaders.
- Organizational structures may also play a role. For some organizations — particularly those that have built through mergers and acquisitions or that are global — internal silos can leave technology and data platforms segmented across the company. "Our biggest challenge is we have so many systems within the company," said the director of risk management and insurance at a global auto industry company. The time it takes to gather data from multiple functions across geographies can be daunting, he said.

So here, again, is a chance for risk professionals to play an important role in connecting parts of the organization to executive decision makers. "Risk management has got to be the one that raises that red flag and says: 'Everybody, here's what we all need to look at, let's make sure we're all going in the same direction,'" said a risk executive at a manufacturing supplier. As risk management is increasingly turned

FIGURE 9 Data and Analytics Use

MY ORGANIZATION WOULD BENEFIT BY IMPROVING ITS USE OF DATA AND ANALYTICS IN THE FOLLOWING AREAS*:



*RESPONDENTS COULD CHOOSE THREE FROM THE LIST.

to for strategic insights, it will benefit by its success in enabling decision making with transparent data and a consistent analytics framework.

We asked survey participants where they would like to improve the use of data and analytics (see Figure 9). Responses were spread within a fairly narrow range among the possible choices. This reinforces a trend for organizations to seek additional support for decision making processes based on data and analytics.

Still, there is a fair amount of impatience and frustration evident in the current state of risk data and analytics:

- Only 23% of survey respondents said that analytics to support strategic decisions will be a priority for their organizations in the coming 12 months.

- Several focus group participants said that some areas of modeling and "big data" are often not used properly. "There are lots of people who are very bright, very capable, and want to use the analytics to advance a particular business perspective. But, they have a tendency not to connect the dots," said the director of risk operations at a major retailer. "They're not seeing beyond their immediate silo, they're not using the data to generate a larger strategic picture."

- Others said there are issues around organizational culture. For some, that means cost: "Everybody wants to do it as cheaply as possible so that everybody keeps looking for one piece of software that is going to provide the information for everybody," said one focus group member.

- For others, changing demographics create a technological disconnect between older employees and younger ones. "I see a generational gap that exists within the organization and the ability to use technology," said a manufacturing company risk director. "While younger workers are keen on technology, they lack the organizational history that will let them best apply it," he said.

But any frustration stems largely from a feeling that there is much to be gained by getting data and analytics right, a point backed up by investment predictions. Over the next two years, 42% of organizations expect to increase the level of investment in risk analytics, according to our survey, with 57% saying it would remain flat. In only one other area — training — did more respondents (46%) expect to see investments increase.

"We had a recent conversation with our information security officer and walked through cyber modeling with him," said the risk manager at a financial institution. "He thought it was a very interesting way to think about a cyber event for our organization. It's interesting to see those things becoming more a part of the conversation."

BUILDING A FRAMEWORK FOR MANAGING CYBER RISK

Our survey again highlighted the hyper-focus on cyber risk: More respondents listed it as the top priority for 2015 than any other area of risk management.

Top Five Risk Management Priority Areas in 2015

1. Cybersecurity.
2. Identifying and improving risk management best practices.
3. Risk training and awareness.
4. Insurance program optimization.
5. Claims management.

"Cyber scares us to death." That was the blunt assessment from the vice president, enterprise risk management, of a US-based, international food corporation that has recently expanded from being only a supplier into retail.

Many organizations are reaching the point in managing cyber risks where they see the goal as beyond prevention. They realize now that, given the resources hackers have at their disposal and the growing connectivity of the oft-cited "internet of things," cyber events cannot always be prevented. The definition of cyber risk has expanded beyond the loss of personally identifiable information. Today's criminals may aim for extortion, reputation smears, denial of service, vandalism, and more. At the same time, employee errors, unforeseen catastrophes, suppliers' IT breakdowns, and the like can damage systems and expose businesses to reputation damage, regulatory scrutiny, stakeholder dissatisfaction, and severe financial losses.

CONTRADICTORY BEHAVIOR

And yet, perhaps because it is evolving so rapidly, we saw some contradictions in the actions that organizations have taken to date with respect to cyber risk (see Figure 10). For example:

- 82% of respondents said they have conducted assessments to determine their vulnerability to cyber-attacks and IT outages. Yet, less than 40% said they have modeled potential losses. Which begs the question: What was the point of the assessment if they haven't modeled the impact?

- Similarly, 80% said they have allocated resources for prevention, preparation, and response. And yet, 70% have not planned for a cyber extortion event, and nearly 60% have no formal communications plan for a cyber event. What, then, are the resources going toward?

- Finally, 80% said they have reviewed their insurance policies for coverage gaps. But Marsh data shows that fewer than 25% of clients buy standalone cyber coverage. So are companies identifying limited coverage and then still not purchasing?

We also looked at the results through an industry lens.

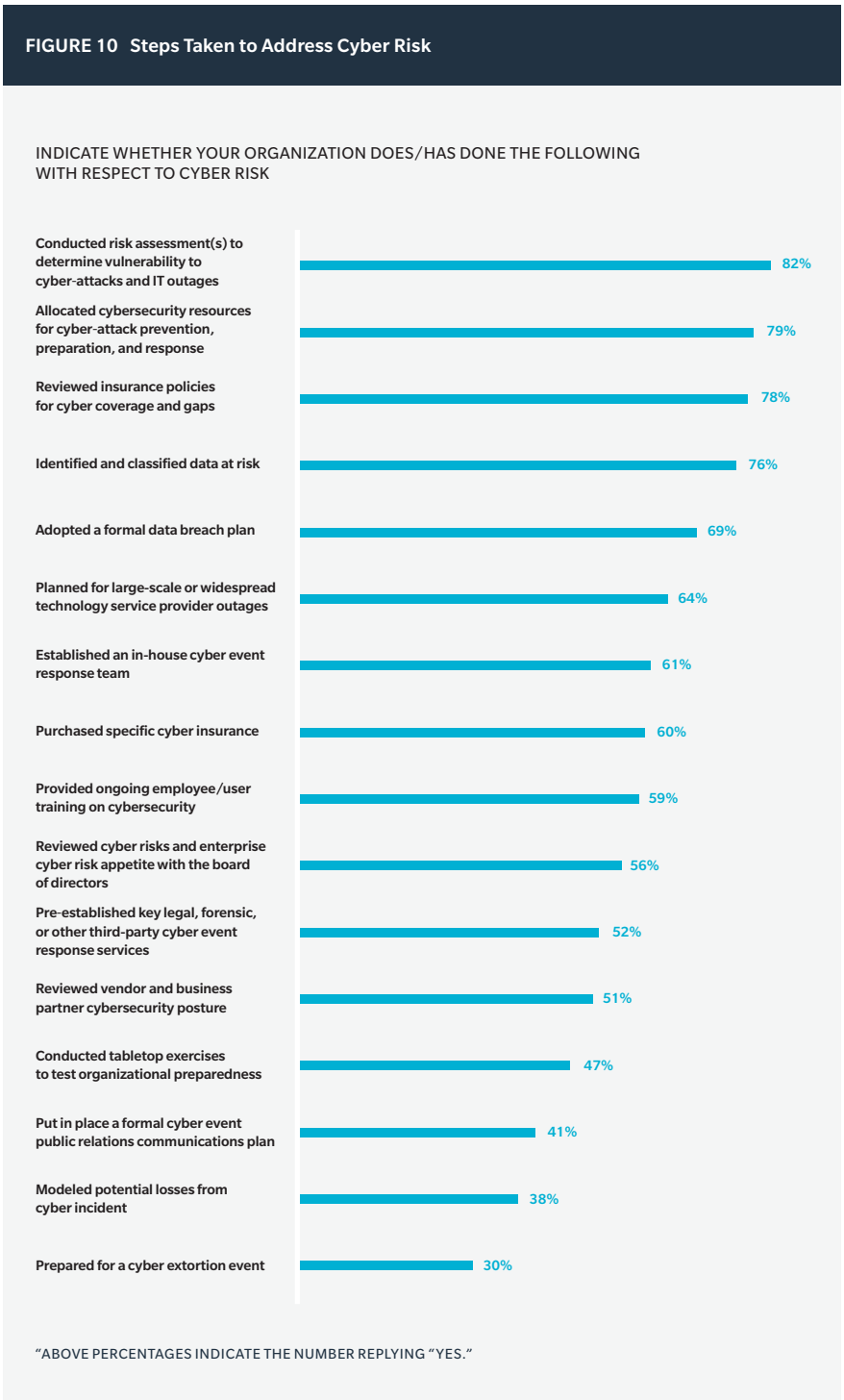
Financial institutions have generally been on the front lines as far as cyber-attacks, so it was not surprising to see that a higher percentage (82%) reported adopting a formal data breach plan compared to all other industries (65%). In most areas in the survey, financial institutions reported higher levels of action around cyber risk. However, one area in which it fell slightly below all other industries was modeling of potential losses: 36% of FI organizations reported taking that step compared to 38% in all other industries.

Health care organizations, similar to financial institutions, generally reported a higher level of actions taken regarding cyber risks than other industries. The health care risk professionals in our focus group cited recent high-profile breaches as being prime motivators: "It would be a gross understatement to say that our organization is focused on cybersecurity related to recent incidents. There's a lot of attention from the board on down." Reviewing the cybersecurity measures at vendor and business partners is one action that health care organizations are more likely to be taking (64%) than in all other industries (48%).

Retail organizations were generally in line with financial institutions and health care organizations regarding items such as planning for data breaches and identifying data at risk. One surprise was that only 53% of retailers reported providing ongoing employee/user training on cyber security, while 59% of respondents overall said they are doing so. And although the number of retailers (50%) saying they put in place a formal cyber-event communication plan was higher than the average (41%), it still seemed low given the spotlight retailers tend to find shining on them when an event occurs.

The above findings reinforce those of other recent surveys. For example, in the 2015 *AFP Risk Survey* — conducted in conjunction with Oliver Wyman, a Marsh sister company — only 40% of respondents said they are developing or updating cyber response plans as part of their actions to respond to and mitigate cyber risk. Instead, the AFP survey found finance professionals pointing primarily to technological fixes. That survey also highlighted a number of difficulties in meeting challenges to reduce an organization's vulnerability to cyber risks — primarily the implementation of a risk assessment process to identify vulnerabilities and ensuring proper levels of encryption are implemented across external networks.

FIGURE 10 Steps Taken to Address Cyber Risk



59% of respondents have no formal cyber event communication plan.

HOLISTIC RESPONSE TO CYBER RISK

The focus on cyber risk is a boon to risk professionals working to boost risk management's strategic partnership with their overall business. Many are now building a holistic framework for managing cyber risk. For example, some report creating cross-functional committees focused solely on cyber issues.

"About eight months ago we started a corporate cyber risk committee, which is basically the heads of every single department that we have and including our COO and our CFO. And we have created local subcommittees as well at all our properties," said a gaming industry risk professional. For organizations currently without an executive risk committee, these risk-specific committees ultimately can be leveraged to address a broader range of risks.

Several focus group members said the elevation of cyber can be seen in increased engagement at every level, from operations to risk committees to boards: "I think the board has been a lot more astute into really understanding the exposure we have to cyber. ... They are very concerned about what happened to some of the companies that have had breaches, and the changes in their boards because of that," said the risk professional at a gaming organization.

And the definition of what is at risk is broadening, according to focus group participants:

- A major auto manufacturer is looking at the technology in cars as customers demand high levels of connectivity in their vehicles.
- A large school district noted that risks run the gamut from giving internet access to children at nearly 500 campuses to maintaining health care records for thousands of employees.
- A financial services provider said a major strategic focus is to anticipate cyber risks elsewhere. "There is a lot of focus on staying abreast of cyber events happening in any industry, and then evaluating how or if that could affect our industry," said one focus group participant.
- A hospitality and gaming company is concerned about protecting the confidentiality of its customers.
- And a food company is particularly concerned with aligning best practices with its global partners. "The foreign companies and vendors that we do business with do not have the same standards. They do not have the same safeguards."

Our survey results and discussions with risk executives show awareness of the changing nature of cyber risk — it is more than data breaches. There is a growing acceptance that problems are inevitable, be it from hackers or an outage caused by something less nefarious. The need for a holistic organizational response is starting to take shape, but needs more focus. Risk professionals should recognize this as an opportunity to play a guiding strategic role in a high-profile, potentially costly area.

"Cyber scares us to death."

– Risk professional at an international food company.

RECOMMENDATIONS

Following are recommendations for risk professionals and executive management based on this year's *Excellence in Risk Management* report.

- Develop strategies to increase alignment regarding risks and risk management across the organization. This may be as simple as asking executives responsible for different business and resource units what value they would like to get from risk management that they currently are not receiving. Articulate specific alignment challenges and develop potential solutions to close the alignment gap.

- Work within your organization and through networking outside your organization to explore performance measurements that more closely reflect the risk management function's strategic value. Consider a performance measurement such as identifying areas in which risk management is least effective as a goal for improvement.

- Form a risk committee of interested individuals to formalize risk reviews, if one is not already in place. Review the composition of risk committees, and those involved in risk management strategy development and assessments/responses to include those responsible for strategy planning and execution. Broaden involvement beyond safety, business continuity, and legal in all risk management protocols.

- Build a broader framework around cyber risk that identifies intellectual property assets as well as data at risk, models potential circumstances and consequences, and involves all areas in response planning — including vendors and suppliers — that may have responsibilities before, during, or after an event.

- Use this report and others, such as the WEF *Global Risks* series, to help stimulate and guide discussions about the future of risk management.

About Marsh

Marsh is a global leader in insurance broking and risk management. We help clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 27,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global team of professional services companies offering clients advice and solutions in the areas of risk, strategy, and people. With 57,000 employees worldwide and annual revenue exceeding $13 billion, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a global leader in providing risk and reinsurance intermediary services; Mercer, a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a global leader in management consulting. Follow Marsh on Twitter @MarshGlobal.

About RIMS

RIMS, the risk management society™, is a global not-for-profit organization representing more than 3,500 industrial, service, nonprofit, charitable and government entities throughout the world. Dedicated to advancing risk management for organizational success, RIMS brings networking, professional development and education opportunities to its membership of more than 11,000 risk management professionals located in more than 60 countries.

For more information, visit www.RIMS.org.

About this Report

This report is based on more than 300 responses to an online survey and a series of focus groups with leading risk executives conducted by Marsh and RIMS in February 2015.

For further information about Marsh, please visit marsh.com.

For further information about RIMS, please visit rims.org.

MARSH IS ONE OF THE MARSH & McLENNAN COMPANIES, TOGETHER WITH GUY CARPENTER, MERCER, AND OLIVER WYMAN.