The EY 2017 Insurance CRO Survey: Shifting from Defense to Offense

By Chad Runchey and David Paul

EY's survey of North American chief risk officers revealed a shift in their responsibilities away from regulatory issues. Chad Runchey and David Paul discuss how they are instead coping with disruption, battling cyber threats and leading the charge on innovation.

EY's Insurance CRO Survey, has for several years, tracked the development of risk management and the changing priorities of the chief risk officer (CRO). The 2017 survey was our broadest ever, with respondents from more than 40 companies.

Previous EY survey reports have described the progress made by organizations and chief risk officers in the development and maturation of enterprise risk management (ERM) capabilities. Particularly since the financial crisis of 2007, companies have installed more formal ERM programs, they have strengthened their risk teams and, in many cases, they have created an office of the CRO (or that office has become more senior and separate within executive leadership teams).

NEW THEMES EMERGING

However, in 2017, as we interviewed participants, we heard of different challenges and new drivers that have the potential to change the role.

It remains true that CROs continue work to embed ERM in operations and to strive for processes that are efficient, accurate, based on sound data, and avoid duplication and rework. But clearly the climate has started to change.

The 2017 survey interviews make it clear that CROs are devoting much less time to regulatory issues. For example, CROs told us that implementing the National Association of Insurance Commissioners' (NAIC) Own Risk and Solvency Assessment by 2017 can now be regarded as "job done" for insurers regulated by state departments of insurance. Some CROs regard their ERM frameworks as advanced or mature.

Responding to the new climate, the 2017 report is focused on the reorientation of the role of CROs and risk functions. The report groups observations under four critical transitions, which some CROs regard as essential next steps. In some cases, these transitions are already in progress, while other organizations are striving to get started.

1. Moving from relative stability to the age of disruption
2. Moving from clear and well-understood threats to emerging and unknown risks
3. Moving from serving as a control function to partnering with the business
4. Moving from the risks of action to the risks of inaction in promoting innovation

Additionally, the 2017 report features an in-depth review of CROs and cybersecurity, which was a major topic of our discussions in 2017 and was the top-ranked risk for many CROs.

COPING IN AN AGE OF DISRUPTION

Our discussions with CROs also explored the theme of disruption. CROs see disruption coming from rapid change in their own marketplace and from the world around them. CROs fear their businesses will be "the disrupted" if companies fail to adapt their businesses fast enough. The questions are, "How can a company be the 'disruptor?'" and "What is the CRO's role in promoting this type of disruption so that the business is protected and can grow?"

When it comes to disruption, CROs are also focused on:

- Challenging whether existing stress and scenarios testing is broad enough to anticipate events
- Asking if stochastic models embrace the true extent of risk, especially relative to the tails of distributions and correlations between risk types
- Confirming that the company has sufficiently detailed response readiness plans and sufficiently robust horizon-spotting capabilities
- Starting to evaluate revolutionary paths, not just evolutionary development (e.g., running scenarios for exiting some markets and entering new ones). If one market is closed, how does the CRO make sure the company is seeking out new markets and finding other sources of growth?

TRANSITION FROM CLEAR AND WELL-UNDERSTOOD THREATS

We asked CROs about how their organizations are "adequately positioned for emerging trends." Many responses stressed the importance and reliance on their emerging risks processes. The report captures what we heard—how this process works, the parties who are involved, the role of risk teams and the CRO and the uses made of the outputs from the process. It also shows the wide diversity of emerging risks on CROs' radar in 2017.

Most CROs see emerging risks processes as clearly necessary, but some admit to shortcomings, especially if the process resides wholly in the first line of business management. Some CROs we spoke to—especially those with more organizational influence—take on the challenge for themselves and their risk teams, verifying that horizon scanning is conducted with rigor and imagination.

CROS AND CYBERSECURITY

Given recent headlines and the severity of cyber threats, it is no wonder that insurance industry CROs rate it as a top concern. What is surprising, however, is that many survey respondents reported their cybersecurity efforts as being in a state of flux.

Many companies have yet to adopt a formal "three lines of defense" approach for cyber risk. The result is considerable variety in the levels of CRO involvement and responsibility for cybersecurity and in the methods for measuring cyber risk, as well as the relationships to chief information officers (CIOs) and chief information security officers (CISOs).

Some CROs in the survey stood out as playing major leadership roles with cybersecurity, but these were in the minority. More CROs reported playing a passive role, though a few had served as temporary "SWAT Team" leaders, troubleshooting in urgent situations and spearheading change management and remediation efforts as circumstances required.

In terms of measurement, companies at least count breaches and some have started to gauge the scope of financial damage, although they acknowledge that operational and reputational impacts may be more severe than financial loss. Cyber risk scores and third-party assessments are being used by a few companies, but overall measurement remains basic, on the evidence of our survey.

Increasing regulatory activity is affecting the approach to cybersecurity at some companies. For example, they may design governance structures to align to future regulations at the state level. CROs are very mindful of the NAIC cybersecurity model law process, even though that process has not finished and will require adoption and enactment by state legislatures across the U.S. However, the potential damage—and even the existential threat—from a cyber event is a much more powerful driver than regulatory compliance.

The Cybersecurity Bottom Line

The increasing severity of cyber risks has been at the forefront of risk management discussions during the last five years. Some participating CROs mentioned that their companies are still reorganizing and stepping up the urgency of their response plans. Some insurers have changed where the prime responsibilities for cyber risks reside, with the CRO and the role of the risk team.

CONTINUED ON PAGE 14

One CRO observed that business units may be equipped to spot local risks and respond incrementally to external change, but may not be capable of spotting or responding to sudden and "macro" changes that impact the whole company.

In fact, some CROs believe they need to be proactive to make sure the organization is innovating and evaluating potential changes in the right direction. This group sees such facilitation not as an "add on" or "optional" responsibility, but rather at the core of their job description.

The most serious risks for a company may include inaction, inflexibility, failure to innovate and a slow speed-to-market.

FROM CONTROL FUNCTION TO PARTNERING WITH THE BUSINESS

- CROs in senior leadership positions (and, in some cases, also leading the strategy function)
- An ethos for the ERM function to promote transparent innovation, rather than constrain it, in interactions between risk and first-line functions
- A CRO focus on communication between businesses, sideways to senior leadership and upward to boards

Several CROs regard themselves as uniquely placed in the development of company strategy. They are independent and, with their second-line positioning, able to take a broad, holistic and enterprise-wide view.

TRANSITION FROM RISKS OF ACTION TO THE RISK OF INACTION

While traditional CROs analyze and monitor current and proposed actions for current business exposures, some CROs are concerned that the risks associated with inaction may be grave. Indeed, the most serious risks for a company may include inaction, inflexibility, failure to innovate and a slow speed-to-market.

It is a particular challenge for CROs to play multiple roles simultaneously:

- Guarding against excessive risk-taking
- Facilitating innovation
- Verifying that a company's capital is prioritized wisely between more and less capital-intensive current business—and between more and less speculative new ventures

This brings up several potential challenges with facilitating "action" in the new world, including:

- The role of risk teams and CROs in product development
- How to launch products with limited data
- The possibilities and challenges associated with having surplus capital

As disruption becomes a dominant theme in so many parts of the business, CROs are working to verify that their companies have sufficient defense and protection from external threats of disruption. But the 2017 survey results make clear that some CROs are going further—playing offense and pushing their companies forward to innovate and disrupt for business advantage.

Chad Runchey and David Paul coordinated the interviews for EY's 2017 CRO Survey and extend their appreciation and thanks to all the companies and CROs who participated and provided the insights collated in the report. This article previously appeared in Insurance-ERM *and is reproduced with permission.* ■

Chad Runchey, FSA, MAAA, is a principal at Ernst & Young. He can be reached at *chad.runchey@ey.com*.

David Paul, FCAS, MAAA, is an executive director at Ernst & Young. He can be reached at *david.paul1@ey.com*.