Article from

Risk Management

May 2019
Issue 44

Chairperson's Corner

By Mario DiCaro

I was recently asked to participate in a survey and specify my opinion on the top five risks from an enterprise risk management (ERM) perspective. I've read the consolidated responses to these surveys many times and contributed to them occasionally. This time the open framing of the question gave me pause. I realized that without context regarding the industry, country or time frame, I was mentally drilling further down into my standard responses to this question.

For example, if the survey had specified "top five risks to property and casualty insurers over the next two years," I would have given a different response than if it had specified "top five risks to the SETI program over the next 30 years." What I came up with was a somewhat sarcastic response that I'll summarize into what I think are the universal risks ERM should monitor:

- The belief that rules keep you safe; and
- The very real possibility of important issues falling through the cracks.

Rules don't keep you safe. Following a rule keeps you safe from the specific danger, or set of dangers, the rule was designed to protect you from. One of the main rules of driving in the U.S. is to drive on the right side of the road. Suppose you are driving on a two-lane twisting mountain highway. The mountain rises to your right. The oncoming lane is to your left. Beyond that is a thousand-foot drop. At times you can see for hundreds of yards ahead and the turns are safer if you straddle the center lane. What do you do? I often straddle the lanes. This leads to screams of terror from my children, who understand the rule that one should drive on the right side of the line but have no experience driving. Maybe I'm wrong, though, and should just slow down. What do you do?

I recently attended a presentation by a power-generating-facilities expert. The subject was cyber risk. He had numerous examples of policies that were in place securing the networks of these companies. The audience raised a couple of real-life examples of breaches that had occurred. He responded by pointing out the specific failures of adherence to rules that had accompanied those breaches, but he maintained his view that the facilities were safe. A few months later I was reading in the newspaper of a widespread hacking campaign that had breached multiple power-generating facilities by targeting weak points in the networks of various contractors servicing the facilities. No number of rules can stop these sorts of deliberate attacks. Only with very vigilant, creative, engaged employees would you stand a chance. Even then things will still get through the cracks.

Which leads me to the next type of risk: things falling through the cracks. Or, in the case of cyber risk, things being extracted through the cracks. In volleyball sometimes two players will watch as the ball lands between them. From a corporate perspective, the ball is likely invisible if it is falling between two different zones of responsibility. Not only does nobody call it, but nobody can see it. ERM teams should be actively looking for intersecting zones of responsibility to see that risks aren't falling through the cracks. ERM teams are often referred to as the second or third line of defense. If you find yourself on one of these teams, I recommend you take responsibility for the spaces between those positioned on the first and second lines. Some examples of such issues are fungibility of assets, correlation or clash of claims across lines of business and efficient use of reinsurance. You may be the only team in the company in a position to identify and quantify these issues. ■

Mario DiCaro, FCAS, CERA, MAAA, is VP, capital modeling and analytics, at Tokio Marine HCC. He can be reached at *mdicaro@tmhcc.com*.