Risk Management

JOINT RISK MANAGEMENT SECTION

ISSUE 41 • MARCH 2018

Conversation with a CRO: An Interview with Nick Silitch

Page 6

3 **Chairperson's Corner**
By C. Ian Genno

4 **Editor's Note**
By Baoyan Liu (Cheryl)

5 **Staff Corner**
By David Schraub

6 **Conversation with a CRO: An Interview with Nick Silitch**

10 **2018's Most Dangerous Risks for Insurers**
By Dave Ingram

12 **The EY 2017 Insurance CRO Survey: Shifting from Defense to Offense**
By Chad Runchey and David Paul

16 **Optimal Level and Allocation of Cybersecurity Spending**
By Shaun S. Wang

19 **ERM in Five Words Part 2: Alignment, Adaptability and Resilience**
By Dave Ingram

23 **Recent Publications in Risk Management**

Risk Management

Issue Number 41 • March 2018

Published three times a year by the Joint Risk Management Section Council of Canadian Institute of Actuaries, Casualty Actuarial Society and Society of Actuaries.

475 N. Martingale Road, Suite 600
Schaumburg, Ill 60173-2226
Phone: 847-706-3500 Fax: 847-706-3599
www.soa.org

This newsletter is free to section members. Current issues are available on the SOA website (www.soa.org).

To join the section, SOA members and non-members can locate a membership form on the Joint Risk Management Section webpage at www.soa.org/jrm

Publication Schedule
Publication Month: August 2018
Articles Due: April 24, 2018

2018 SECTION LEADERSHIP

Chairperson's Corner

By C. Ian Genno

As you open the pages of this issue of the newsletter, I'd like to take a moment of your reading time to highlight some of the initiatives the Joint Risk Management Section has been pursuing since my last update in the December 2017 issue.

Kailan Shang has completed a research paper on "Effective ERM Stakeholder Engagement," with project guidance and funding from the section. By surveying the experiences of risk management professionals in engaging ERM stakeholders (in board, senior management and three lines of defense roles), a number of valuable insights emerge—including perspectives on understanding stakeholder needs, ERM communication strategies, quantifying the benefits of ERM investment, creating accountability to ensure risk policies are followed, and assessing and improving an organization's risk culture. Supporting examples illustrate how to apply the concepts effectively in practice.

Other research work includes our periodic Emerging Risks Survey, and our collaboration on the Actuaries Climate Index to help address the needs of actuaries involved in the modeling and pricing of catastrophic risk coverage. Both of these research concepts are gaining significant attention in the business community and the broader public arena. You can read more on risk management research at *www.soa.org/jrm*.

Planning and coordination work continues for risk management related sessions at a number of upcoming actuarial conferences. Section council members provide perspective and input on themes, relevant topics and speakers; and in a number of cases the section also provides sponsorship support to help ensure the financial viability of conferences and reduce the registration costs borne by participants.

We are developing our 2018 series of webcasts, providing members with a quick and cost-effective way to gain access to CPD opportunities on current issues, while eliminating travel time and cost. The section is also now offering members free access to section-sponsored webcasts from 2015 and 2016 (one year or older). The webcast recording offerings will be updated on a quarterly basis. Section members can access the free webcast recordings by logging into the Joint Risk Management Section Community which is housed at *https://engage.soa.org*

This year's ERM Symposium is fast approaching—April 19–20 in Miami. If your calendar is open and you haven't yet registered, I encourage you to look at the lineup of topics and speakers. The symposium offers a wide range of content and perspectives, and a valuable opportunity to engage in informal networking conversations with a broad cross-section of your peers in risk management. You can find further information at *www.ermsymposium.org*.

In addition to planning different ways to deliver CPD content in person and online, we're considering ways to better facilitate local networking opportunities for section members, whether through sponsorship support or helping to coordinate speakers on risk management topics for local events.

And as always, we continue to focus our time and attention on this newsletter. I would like to acknowledge the significant initiative taken by the editors and staff to source interesting and relevant articles; without their ongoing effort, this newsletter simply wouldn't be possible. I hope you'll enjoy reading it today. ■

C. Ian Genno, FSA, FCIA, CERA, is the head of the Mortgage Insurance Group at the Office of the Superintendent of Financial Institutions, the federal banking and insurance regulator in Canada. He can be reached at *ian.genno@osfi-bsif.gc.ca*.

Editor's Note

By Baoyan Liu (Cheryl)

The modern insurance industry started in the 17th century, with the first fire insurance company officially established. The industry expanded into property lines, life insurance, accident, and health insurance, while its business model became more and more sophisticated over the last 400 years against waves of attacks by risk demand incurred from social development. Nowadays in 2018, the insurance industry is facing a new wave of disruption from technology evolution as disruptive newcomers and digital transformation redefine the marketplace.

Technology disruptions on insurance product pricing, underwriting, operations, business conduct, and customer expectations have become the top concerns of the industry. And associated with the digital platform transformation, cyber landscape has also been at the forefront of risk management discussions. In this first issue of *Risk Management* in 2018, I'd like to share articles with a focus on the top risks in our industry.

First, the Joint Risk Management Section is pleased to announce the start of a new feature series, "Conversation with a CRO," where the top risk practitioners in the insurance industry offer insights into the major issues facing the industry, through interviews with our experienced partner actuaries. Our first guest in the CRO conversation is Nick Silitch from Prudential Financial. He shared his perspectives with Tony Dardis and Awa Kone on the topics of risk culture, the use of economic capital, and the role of actuaries in risk management.

Good risk management requires striking a balance between following the wisdom of the market and relying on your own insight. Dave Ingram from Willis Towers Watson provides a summary of "2018's Most Dangerous Risks for Insurers" in the survey they performed. As insurers become more digitized, cybersecurity & cybercrime is constantly rated a top risk and it has by no means finished evolving. Traditional risk concerns such as off-track strategic direction, natural catastrophe claims, competition and pricing/product risk, also have their places in the Top 10 risk list.

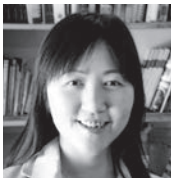
For several years, EY's Insurance CRO Survey has tracked the development of risk management and the changing priorities of the CRO. In this issue, Chad Runchey and David Paul highlight the key findings in "EY Insurance CRO Survey—Shifting from Defense to Offense."

Cyber risk and cybersecurity has been ranked as the number one risk two consecutive years in the most dangerous risks survey by Willis Towers Watson, and as the top concern rated in EY's insurance industry CRO survey. As insurers are more susceptible to cybercrime, heightened cybersecurity requires more efficient IT system investment. Globally, firms have spent billions of dollars on advancing their internal system defense against cybercrime. Dr. Shaun Wang from Nanyang Technological University presented his research on "Modeling Optimal Level and Allocation of Cybersecurity Spending" at the 2017 Actuarial Research Conference (ARC). We're pleased to invite Dr. Wang to share a summary of his presentation with our readers in this issue of *Risk Management*.

Effective ERM can be a lengthy discussion. Dave Ingram shows us this in a series of two articles, "ERM in Five Words." Part 1 was published in our December 2017 issue of *Risk Management*. And it describes resilience, transparency and discipline. Continued in this issue, Part 2 will illustrate the importance of alignment and adaptability.

As always, we provide a list of recent articles and papers that may be of interest to our members. These pieces can provide further information on a broad range of topics.

I would like to give a special thank you to David Schraub and Kathryn Baker for helping me pull together this March issue of the newsletter. Enjoy reading! ■



Baoyan Liu (Cheryl), FSA, CFA, is senior manager, risk management at FWD Life Insurance Company (Bermuda) Limited in Hong Kong. She can be reached at *cheryl.by.liu@fwd.com*.

Staff Corner

By David Schraub

The ERM Symposium is the Joint Risk Management Section's "baby." And just as it takes nine months from conception to delivery, we take just as much time to grow and nurture this symposium for our attendees. This year, the ERM Symposium will be ready on April 19 for all to experience and enjoy.

About nine months prior to the meeting, the dedicated committee of volunteers is formed. In doing so, we look for a diverse makeup—U.S. and Canadian members with both P&C and life backgrounds, veteran members, and also new blood. The location for the meeting has been set. Discussions start on the philosophy of the meeting—the unique message we are looking to weave through the meeting to make the trip to the ERM Symposium a renewed experience for our attendees. This year, we are looking for fresh content that has not been presented in other venues, as well as looking to dedicate a significant time for Q&A to increase audience participation.

About seven months out, the committee articulates the number of sessions needed for each broad theme and issues a call for proposals to leverage potential great ideas existing outside the committee. About four to five months prior to due date, sessions or the proposals are selected. Presenters are notified. Recruiting starts to pick up, leveraging the proposals but also the collective knowledge of committee members. Similar themes are merged and necessary counterpoints are provided. Sponsorship packages are getting finalized.

About three months prior to due date, the skeleton of the symposium is getting shaped. This means staff is gathering (almost) final titles and descriptions for all breakout and general sessions. This also means the session line-up is getting finalized, where we ensure each time slot has a variety of session options for each type of potential attendee—for a life technical actuary to a P&C C-suite risk manager and everything in between. We are also ensuring two breakout sessions that will appeal to the same audience do not conflict. We reach out to potential sponsors and articulate the benefits of the visibility at the ERM Symposium.

Some staff make a visit onsite to better visualize the space for sponsor table tops, signage and other room settings.

About two months out, the last remaining open slots should get filled with speakers. Marketing emails should be flying. Sponsor contracts finalized and we monitor the registration in order to estimate the crowd for each breakout room. Will a setting with five round tables fit this room? Do we have space for the arm chairs and the podium for the CRO panel?

The last month should be much quieter for staff, as the main tasks are to monitor the registration and the presentations coming in . . . unless there are emergency issues to deal with, with a session to be built using our backup plan.

There is much planning that both committee and staff do to ensure a smooth delivery and a great experience for our members. The committee is a group of 15 volunteers, and many staff members at the CAS and SOA work jointly on the project. The SOA ran the symposium in 2017 and will do so again this year, passing the baton to the CAS for 2019 and 2020 to perform the majority of these tasks. This alternating pattern is pretty seamless, proving once again the solid partnership between our actuarial organizations to deliver great content for the common benefit. This is what the Joint Risk Management Section is all about!

We hope to see you at this year's ERM Symposium! ■

David Schraub, FSA, CERA, MAAA, AQ, is staff fellow, risk management at the Society of Actuaries. He can be reached at *dschraub@soa.org*.

Conversation with a CRO: An Interview with Nick Silitch

Nick Silitch, Chief Risk Officer, Prudential Financial

The Joint Risk Management Section is pleased to announce the start of a new feature series, "Conversation with a CRO." Going forward, each issue of *Risk Management* will include an open and candid Q&A with one of the top risk practitioners in the insurance industry, offering insights into the major issues facing the industry and how the very best in the industry are addressing the issues.

In this, the first in our new series, *Risk Management* is honored to have been given the opportunity to interview Nick Silitch, CRO of Prudential Financial. Never one to hold back on expressing a view, and always ready to engage in a lively discussion, our interview with Nick held much excited anticipation, and we were not disappointed.

Nick was interviewed at his office on Oct. 23, 2017 by Tony Dardis and Awa Koné, of Milliman, Inc.

Nick Silitch is one of the most respected and well known risk practitioners in the financial services industry. As CRO of Prudential Financial, Nick oversees Prudential's risk management infrastructure and risk profile globally. Nick chairs the organization's Enterprise Risk Committee that evaluates current and emerging risks relevant to the company, and is a member of Prudential's Senior Management Council. Nick joined Prudential in 2010 after many years in the banking industry, including nearly 30 years at the Bank of New York Mellon, and is unique in that regard having held senior management positions in both the insurance and banking sectors.

In this wide-ranging discussion with Nick, we were keen to get his perspectives on the topics of risk culture, the use of economic capital, and the role of actuaries in risk management, which were all topics on which Nick had many interesting perspectives.

Q: What are things that can be done to ensure a successful "risk culture" in an insurance organization? What can CROs be doing to make risk management part of their company's strategic decision making?

A: I don't believe in having a risk culture. What companies need to do is start with a foundation that establishes a *company-specific, company-wide culture whereby an appreciation of the value of risk management runs throughout the DNA of the company*. And flowing from that, all strategic decisions then reflect consideration of the balance between the risk profile and opportunity cost associated with that decision and the potential return. If you have a culture that embraces risk management, you will have a chance to be able to grow a healthy organization that actively considers risk and return as it moves forward, which is a good framework for a financial company.

An example of this at Prudential is our risk appetite, which has been bought into across the organization, so there is a common goal in optimizing strategies across multiple financial lenses, whether statutory, economic, or liquidity for the benefit of

shareholders and other key stakeholders. The risk function acts as scorekeeper and stage setter for the risk appetite, but it is owned by the collective organization: the businesses, corporate functions and the board. As a result, the risk function is integral to and becomes involved early on in strategic discussions. For example, as soon as the company starts to consider a new acquisition or a new product, we start asking how this fits into our overall risk appetite.

Q: How do you know then that you have the right culture?

A: I live it every day. Here at Prudential, we truly have an open door policy where everyone is encouraged to speak up. It is a remarkable privilege to work in and be responsible for continuing to cultivate such a healthy environment.

One thing for sure is that knowing you have the right culture is not a matter of ticking the boxes. It's not something you can test or manage to. You could try coming up with say five to six attributes for a successful culture that incorporates risk, but the danger in that is you manage to these attributes and then lose the soul of your culture. You know you have a great culture if whenever confronted with uncomfortable decisions the organization makes the right one. If you are fortunate enough to have this type of culture, the worry is that it could change. As a result, boards, senior managers and other stakeholders need to keep a careful watch on it so that the core of the culture is open dialogue and an active consideration of risk and return.

Q: What role can economic capital (or internal capital) have? What are potential barriers to a successful economic capital program and how can insurers overcome them?

A: The concept of economic capital has been amongst the most misused ideas in finance over the last twenty years. The notion that the modeling of your risks to a certain confidence interval would allow you to be able to equate a dollar of market risk to a dollar of investment, insurance or operational risk is appealing, yet largely unattainable, and of modest use even if successful. The amount of data that we have on many of the risks that we take does not support precise 5 in 10,000 type tail measurements without making heroic and often faulty assumptions. Furthermore, the historic relationships of these risks to one another can break down as tail outcomes are explored.

The value in the exercise of modeling your risks is the understanding that is gained in the shape of the distribution and the role that each input can play in the shaping of that tail. Broad understanding and agreement (line businesses, board and corporate functions) as to the nature of the risks that you take is critical to developing an open, transparent risk dialogue and allowing the organization to collaboratively engage in the management of risk and return. For this reason, economic capital models are important components of the risk management tool box, but must be partnered with deterministic stress testing and an understanding of statutory capital and liquidity implications for an effective risk management framework.

Only when understanding this complete picture can the organization endeavor to optimize outcomes for all relevant stakeholders.

Where economic capital can be useful on its own merit is as a tool for the pricing of risks, ensuring that the economic risk and return profiles stay balanced as we seek to optimize across, largely more conservative, statutory capital requirements.

Q: Do you have priority in your risk appetite limits?

A: We have a risk appetite statement, not limits on risk appetite. It is a high-level idea of how we want to operate the company during periods of stress. Then, we develop financial metrics as interpretations of these high-level ideas and set risk-type limits so we can stay within the desired parameters. We have board limits and operating limits. Our operating limits leave enough room so there is little danger of breaching board limits.

You know you have a great culture if whenever confronted with uncomfortable decisions the organization makes the right one.

Q: Actuaries already play a role in the risk management arena, but could probably do more. How do you see the role of actuaries in this space?

A: Of course, there is a huge role for actuaries in the insurance industry, and I don't think actuaries can do a better job than they have been doing in their fields of expertise. *Being an actuary is its own highly specialized skillset* and while there is tremendous value to the core competency it doesn't mean you are qualified to practice as a risk professional. For instance, a highly qualified investment professional doesn't equate to an investment risk professional, a markets professional doesn't equate to a market risk professional and an actuary doesn't equate to an insurance

risk professional. Each skillset is a critical underpinning to being a strong risk professional, but you must also possess other skills sets. And this is because risk management at the core requires a slightly different focus. Indeed, a good risk manager has to:

- Challenge the status quo;
- Understand the distribution of tail outcomes as well as the best estimate;
- Manage complexity arising from there being multiple agendas around a variety of issues; and
- Understand quantitative and qualitative analytical risk frameworks and the strengths and weaknesses of both.

What's a more useful question to ask here is how well are the actuarial and risk professionals communicating and collaborating? I have an extremely close relationship and open dialogue with our chief actuary, and we have tremendous respect for each other. A healthy dialogue between actuaries and the risk team is essential to the overall management of an insurance company.

Q: Much attention has been given by the industry in recent years to building out model risk management capabilities. What would you view as the key to a successful model risk management program?

A: Model risk for banking is high touch and predictive, which is different than the insurance industry. However, in insurance the rigor in actuarial models is tested regularly and fairly rigorously. Every year there is a model validation process with the auditors and with assumptions unlocking. Therefore, in essence, the core principles of SR 11-7 have existed for years within the insurance accounting, actuarial and financial reporting frameworks. As a result, companies need to be careful to build model risk programs that consider existing strengths and build enhancements around documentation and rigor.

Also critical for model risk, similar to other risk, is the maintenance of open and transparent dialogue around the development and use of models, and the incorporation of models into our business plan. Strong, transparent governance of assumptions and key model components is essential.

Q: Cyber risk is another "operational risk" that has gained increasing focus in recent years. What would you view as some of the biggest issues around cyber risk and how to best manage these issues?

A: Cyber risk is constantly changing and is a focus for a lot of people on both sides.

In this day and age, you have to assume that anybody can possess personal information about other individuals, making the verification of customers' identities more difficult.

Banks are losing a lot of money due to cybercrime every year. Additionally, the cyber threat has evolved over time. It used to be that cyber criminality was focused on individuals. But, over the past decade or more, we are seeing hackers getting more sophisticated and going after companies. As an industry, we invest a lot of resources in this risk. But, the game is constantly changing and the bar will continue to rise. This is why we—and the industry at large—continue to stay focused on the evolving cyber landscape. If this escalation continues unchecked, at some point firms may collectively consider changing how they engage with customers.

Q: Since we are on the topic of threats, in your opinion, what are the main trends in risk in the next three to five years that insurance companies will be facing?

A: Evolution in the uses of data, digital and technology platforms are going to change business models—how we underwrite, how we service customers—and as that happens, there will be operational and products risks.

Advancements in genetics and disease management might make for a different world—influencing mortality and longevity at the extremes in addition to bringing about complex moral and legal issues to consider as well as a potential uneven distribution of information on personal data.

Climate change for P&C. A one degree increase in ocean temperatures changes catastrophe models exponentially.

On the asset side, the industry needs to be cognizant of the fact that the companies we invest in are going through the same economic, political and technological issues that we are facing in the insurance industry, resulting in changing and evolving business models. Therefore, from an investment perspective we have to keep an open mindset. ■

Awa Koné, FSA, CERA, MAAA, is a consulting actuary at Milliman. She can be reached at *Awa.Kone@milliman.com*.

Anthony Dardis, FSA, FIA, CERA, MAAA, is a consulting actuary at Milliman. He can be reached at *Anthony.Dardis@milliman.com*.

CERA

Chartered Enterprise Risk Analyst

CREDENTIAL

Meeting the Global Needs of Risk Management—the CERA

The way they think, the skills they bring, the roles they play. The Chartered Enterprise Risk Analyst (CERA) is a unique blend of the quantitative and the qualitative, combining actuarial discipline with the ability to think critically and creatively about risk, enterprise wide.

It's a level of expertise that can only come from the CERA credential from the Society of Actuaries—the most comprehensive and rigorous available. With a deep understanding of enterprise risk management and ethical standards that are beyond compare, the CERA is the risk professional that organizations trust to take them into the future—turning data into decisions to the benefit of their business.

The ERM Experts—the CERA

CERAnalyst.org

SOCIETY OF ACTUARIES®

2018's Most Dangerous Risks for Insurers

By Dave Ingram

Editor's Note: A previous version of this article appeared in the Willis Towers Watson Wire blog.

Good risk management requires striking a balance between following the wisdom of the market and relying on your own insights. Each year, you need to look at the risks your company is taking and decide if any of them have become more dangerous than they were last year. Also, if there are any new risks coming over the horizon, they should be moved from "emerging" to a place on the list of "presenting" risks.

The following is a version of that process. We provided insurance industry professionals a list of about 70 risks that we had seen on the risk registers of insurers in 2017. Over 230 people responded and ranked over 8,000 pairs. Over twenty percent of the respondents were actuaries and more than half were from U.S. property and casualty insurers. This was the second time that we conducted this survey, so we are able to garner insight into how priorities have changed since last year. The results of last year's survey can be found at *https://blog.willis.com/2017/01/2017-most-dangerous-risks-for-insurers/*.

We found that insurers' concerns have shifted. In 2017, other than the top entry, cybersecurity and cybercrime, most of the concerns were the usual suspects—the traditional risks that insurers have always faced—pricing, IT, competition, underwriting, regulations, investments, and catastrophes.

For 2018, the responses suggest that many insurer managers (those who responded) are concerned that the industry is now closer to becoming the next victim of the modern wave that has emptied out shopping malls and closed countless book stores. Risks in the top ten now include: disruptive technology and customer needs not served by traditional approaches. And, most notably, there is less confidence in management's ability to find its way through these problems; the risk of strategic direction & opportunities missed moved up from 8th place to 3rd.

So here are the top ten risks from the survey. You can use this list and its ranking to challenge your own list of top risks.

1. **Cybersecurity & Cybercrime** (1st in 2017)
   Cyber has appeared at the head of both emerging risk and presenting risk lists in the past year. Risk managers feel that cyber is a major presenting risk and that it has by no means finished evolving. As insurers grow their business operations to become more digitized, they also grow more susceptible to cybercrime and require heightened cybersecurity. In addition, this operational risk may be on the top because of the heavy news coverage of a relatively small number of major incidents.

2. **IT/Systems & Tech Gap** (3rd in 2017)
   Most insurers that we talk to have just completed, are in the middle of, or, are planning a major systems overhaul. There is a fear, however, that all that IT updating requires a constant and expensive effort to keep up. But, if information technology systems are not up to par, insurers run the risk of not being able to satisfy customer service expectations. This is both an operational risk and a strategic risk: the amount of investment in computer systems is the strategic issue while the successful operation of those systems is operational.

3. **Strategic Direction & Opportunities Missed** (8th in 2017)
   Respondents show a lack of confidence that management can get it right. They are afraid that top management will take the company off in a rush—but in the wrong direction, while leaving valuable options on the table. This is, of course, a strategic risk and its position on this list indicates that respondents feel that top management may be too much in the weeds and not enough in the clouds.

4. **Pricing & Product Line Profit** (2nd in 2017)
   Insurance has always been a business where sales are made and prices are fixed before the cost of goods sold (claims costs) is known. The data analytics revolution ties this risk

firmly to the technology issues. This is an insurance risk and if ever it falls outside of the top 10 risks for any individual insurer, it is a clear indicator of impending doom.

5. **Runaway Frequency or Severity of Claims** (19th in 2017)
   Nothing like the highest natural catastrophe claims year to bring about a major jump in this insurance risk. Even if prices and underwriting are just right, bad luck can result in more claims or larger claims than anticipated.

6. **Disruptive Technology** (14th in 2017)
   No one knows what it will be, but many survey respondents are sure that someone, maybe Alphabet or Amazon are quietly developing the insurance company killer app. This strategic risk is a fear that is tied very closely to the next risk.

7. **Customer Needs Not Served by Traditional Approaches** (New in 2018)
   This is perhaps the flip side of the prior risk. For many carriers, the average age of their insureds and agents/brokers increases by almost a full year each year. They fear that the younger generation does not see much value in the insurance products that have been sold for 50 years or more and do not have interest in a sale or claim process that cannot be completed with a few clicks on their smartphones. Another strategic risk that may be linked to aging of insurer management teams.

8. **Emerging Risks** (10th in 2017)
   This risk can be read to mean "We do not know what, but something bad is right around the corner." It may have moved up because of an increasing feeling of ill-defined gloom or the opposite. Emerging Risks may have moved up because there is increasing confidence in management's ability to handle the risks that have been identified.

9. **Competition** (4th in 2017)
   This year, insurers seem to fear tech-based takeover over pressure from a traditional competitor. But the risk at position 9 on this survey still beat out 65 other risks. Competition is always a major risk for insurers because of the high degree of price sensitivity of most customer bases along with low barriers to entry. Many insurers are seeking diversification via expansion out of their traditional geographic footprint which heightens traditional competition. Competition is the classic strategic risk of a capitalistic system.

10. **Underwriting** (5th in 2017)
    Another classic insurance company risk with falling rank. Insurance risks include pricing, underwriting, claims, and reserving. Three of these still fall into the top 10. Reserving does not, coming in 32nd. So respondents still think that it is of high importance to execute the basics of the insurance business. Reserve risk may be seen to be low because of a relatively long streak of reserve releases. That is one of the cyclical parts of the insurance business and it is surprising that insurers do not seem to think that the recent declines in reserve releases is not a sign that the future potential for reserve strengthening is getting closer and closer.

FALLING OUT OF THE TOP 10

Three risks fell out of the Top 10 in 2018:

- **Legislative & Regulatory** (6th in 2017, 11th in 2018)
  Recently completed Federal activity on taxes and lack of activity on the ACA may be the reason for decreased concern about this risk.

- **Natural Catastrophe** (9th in 2017 and 17th in 2018)
  The position of this risk in 2018 may be an example of the Gambler's Fallacy. High losses from natural catastrophe in 2017 do not actually drive down likelihood of large losses in 2018.

- **Investment Market Risk** (7th in 2017, 22nd in 2018)
  This shift in priority for investment risk seems to match with the markets where securities prices are booming and volatility protection is cheap. Sometimes not a great sign, but as JM Keynes said "Markets can remain irrational a lot longer than you and I can remain solvent."

WHAT TO DO WITH THIS INFORMATION?

Think about how this list and the changes from last year compare to your company's thinking. Are there highly ranked risks here that are not even on your risk register or that have a lower ranking? Are you okay with that? ■

David Ingram, FSA, MAAA, CERA, is executive vice president at Willis Re. He can be reached at *dave. ingram@willistowerswatson.com.*

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*.

ERM Enterprise Risk Management Symposium

April 19–20, 2018
Miami, FL

Insight Into The Future

The ERM Symposium provides a dynamic environment for thought leadership, best practices and networking opportunities. Join us for this unparalleled opportunity to learn from leading enterprise risk management professionals.

CAS · Canadian Institute of Actuaries · Institut canadien des actuaires · SOCIETY OF ACTUARIES

ERMSymposium.org

Optimal Level and Allocation of Cybersecurity Spending

By Shaun S. Wang

Editor's Note: The 52nd Actuarial Research Conference (ARC) was held in Atlanta in July 2017, with the theme "Actuarial Research at the Crossroads: Transcending Disciplines." Actuarial educators, practitioners and researchers gathered together to discuss the latest developments and to exchange ideas. In this issue of Risk Management, we are pleased to invite Dr. Wang to share a summary of his presentation at the ARC, "Modeling of Optimal Spending and Allocation on Cybersecurity."

INTRODUCTION

The rising number of cyber breaches has spurred cybersecurity spending by firms. It is estimated (e.g., Gartner, 2017)[1] that globally, the private sector invests $93 billion in 2018 to beef up their internal system's defense against cyber threats. Firms want to know the optimal level and allocation of security investment. Such questions have been extensively explored in the academic literature (e.g. Gordon and Loeb (2002);[2] (Tanaka, et. al (2005)).[3] At the 52nd Actuarial Research Conference, I presented a mathematical model for cyber breach probability as a function of security spending in protecting a firm's ICT systems, and derived optimal level of security investment as percentage of value-at-risk. This article also summarizes the first part of the mathematical model in Wang (2017).[4]

A firm's ICT system generally has an **attack surface** that is exposed to various types of cyberattacks. The attack surface of a firm's ICT system may include open ports on the web and mobile devices, computing services inside the enterprise firewall, and employees with access to sensitive information being socially engineered (see Figure 1). A firm's ICT system is vulnerable to various types of cyberattacks, including malware, DDOS, POS intrusions, phishing and social engineering, advanced persistent attacks, insider and privileged misuse of access, etc.

Firms normally have already invested in some cybersecurity measures to protect its ICT system. A positive security investment, $B>0$, is selected as the *benchmark spending* appropriate for the size of the attack surface. Any amount of security spending Z can be described by the *spending ratio*, $z = Z/B$. For security spending $Z=zB$, we denote the ICT system's cyber breach probability by $v(z)$. At benchmark spending B, we have $z=1$, the firm's ICT system has a cyber breach probability $v(1)$.

One can specify the following regularity conditions for the security breach probability function $v(z)$:

1. $v(0)=1$. When there is zero security spending, there is probability one of being breached.

2. $v'(z)<0$, for $z>0$. As security investment z increases, the cyber breach probability $v(z)$ decreases. In other words, every additional dollar spent yields proportionally less benefit in reduction of vulnerability. A firm ideally should invest into those tools whose return is highest. This return is the rate at which the residual breach probability reduces with incremental increase of the investment z. This rate is non-increasing if the current investment is optimal, as the best protection is acquired first. This intuitive assumption is supported empirically on cross-sectional firm data (e.g., Tanaka et al, 2005).

Wang (2017) considered several classes of cyber breach probability function.

a. The Exponential Power Class:

$$v_{EP}(z) = v(1)^{z^{\alpha}}, \text{ where } \alpha>0 \qquad \text{(eq-3)}$$

b. The Proportional Hazard (PH) Class:

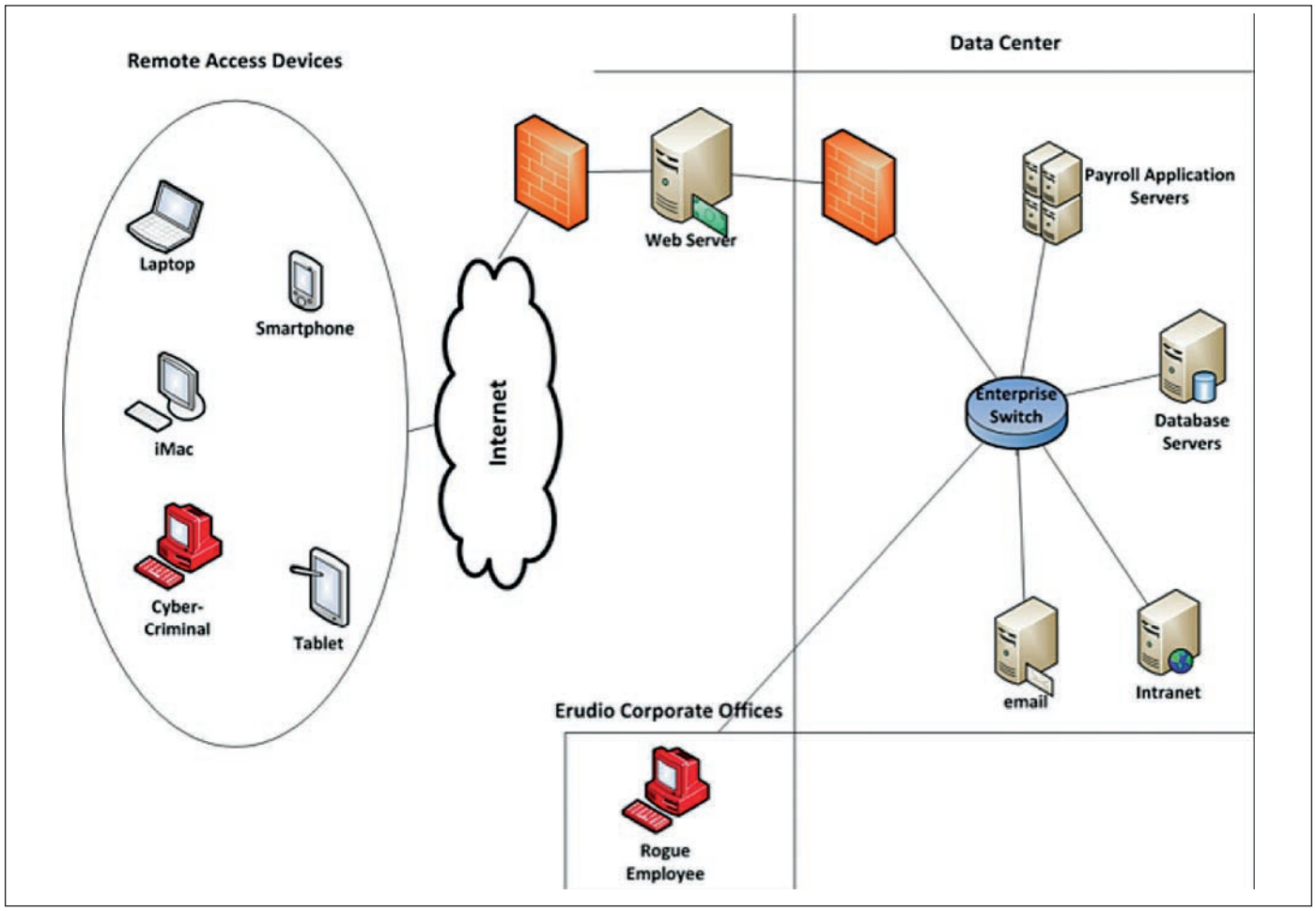
$$v_{PH}(z) = 1-[1-v(1)]^{z^{-\alpha}}, \text{ where } \alpha>0 \qquad \text{(eq-4)}$$

c. The Wang Transform (WT) Class:

$$v_{WT}(z) = \Phi[\Phi^{-1}(v(1))-\alpha\cdot\ln(z)] \qquad \text{(eq-5)}$$

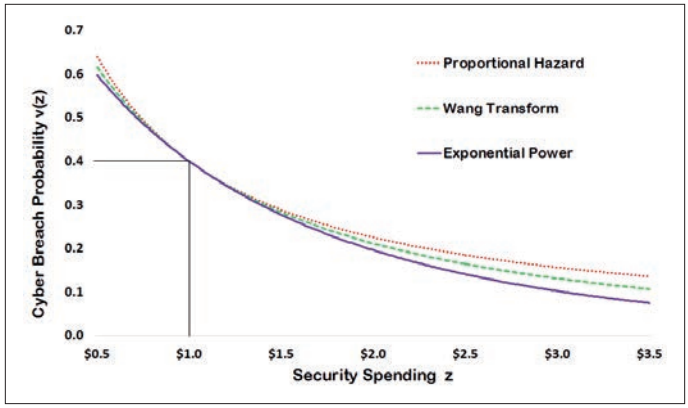
where $\alpha>0$ and Φ is the cumulative standard normal distribution (see Wang, 2000).[5]

Figure 1
An Illustration of an Attack Surface



Source: *http://www.infosecinstitute.com*

Figure 2
Comparison of Cyber Breach Probability Functions



The cyber breach probability function $v(z)$ is said to have an **invariance** property if the same functional form is preserved under a change of benchmark: $\tilde{B}=\tau \cdot B$, for all $\tau > 0$. One can verify that the Exponential Power, the Proportional Hazard, and the Wang Transform classes of cyber breach probability functions all have invariance property, with the functional form and the parameter α remains the same for different choices of the benchmark B.

OPTIMAL LEVEL OF SECURITY SPENDING

Consider a firm's ICT system. Let R represent the potential value-at-risk, or monetary losses and expenses given the occurrence of data breach. Corresponding to the security spending $Z=z \cdot B$, the firm has a cyber breach probability, $v(z)$, and an annual loss expectancy (ALE) of $v(z) \cdot R$. The total cyber cost

to the firm is the sum of security spending Z and annual loss expectancy:

$$\text{Cost}(z) = z \cdot B + v(z) \cdot R$$

The optimal spending ratio z^* is defined such that the firm's cyber cost is minimized at security spending $Z^* = z^* \cdot B$. The optimal level of security spending $Z^* = z^* \cdot B$ satisfies the equation:

$$-v'(z^*) = B/R$$

In the special case of the Exponential Power Class with $\alpha = 1$, the optimal spending ratio has a closed-form formula:

$$z^* = \frac{\ln(R) - \ln(B) + \ln(-\ln v(1))}{-\ln v(1)}$$

Remark: The derivative $-v'(1)$ indicates the *effectiveness* of incremental spending in reducing the vulnerability, at the benchmark spending B.

One can verify that the optimal security investment $Z^* = z^* \cdot B$ has the following upper bounds:

1. For the Exponential Power Class: $Z^* \le \frac{\alpha}{e} \cdot R$
2. For the Proportional Hazard Class: $Z^* \le \frac{\alpha}{e} \cdot R$
3. For the Wang Transform Class: $Z^* \le \frac{\alpha}{\sqrt{2\pi}} \cdot R$

OPTIMAL SECURITY INVESTMENT ALLOCATION TO ADDRESS MULTIPLE AREAS OF VULNERABILITY

Consider that an ICT system which has multiple areas of vulnerability, and cyber breach occurs when a hacker successfully exploits any one area of vulnerability (see Figure 3). We choose the number of areas of vulnerability to be three, although the analysis holds for any number of areas of vulnerability. For each area j of vulnerability ($j = 1, 2, 3$), the benchmark spending is B_j, with a corresponding cyber breach probability, $v_j(1)$. Assume that the organization's security spending $\boldsymbol{Z}$ is allocated to address each area of vulnerability:

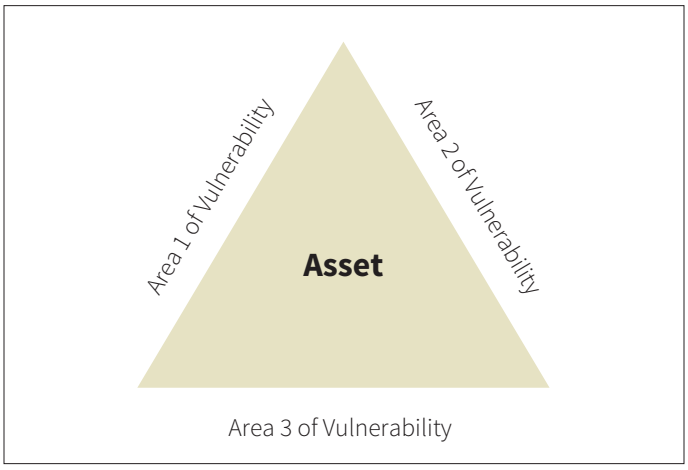
$$\boldsymbol{Z}^* = z_1 \cdot B_1 + z_2 \cdot B_2 + z_3 \cdot B_3$$

We have a competing risk model:

$$v(z) = 1 - (1 - v_1(z_1)) \cdot (1 - v_2(z_2)) \cdot (1 - v_3(z_3))$$

Our model and analysis highlight the importance of security spending to cover the full spectrum of areas of vulnerability; neglecting one area of vulnerability can render the security investment ineffective and wasteful. Moreover, economic value can be gained by differential treatment of the high-value data assets. Firms should give priority protection of their crown-jewel assets (say, by reducing unnecessary connection points and/or by imposing multi-factor authentication).

Figure 3
Parallel Routes or Multiple Areas Vulnerability



The benchmark model in this paper has practical implications. It is advisable for firms to anchor their security spending to some benchmark, and empirically track effectiveness of security spending in reducing vulnerability. For firms, assessing the vulnerability of tis ICT system would require IT expertise and knowledge; identifying the key data assets would require knowledge of the firm's business model. Thus, there is a need for coordination between IT experts and enterprise risk managers. ■

Shaun S. Wang, FCAS, CERA, Ph.D., is professor and director, Insurance Risk and Finance Research Centre, Nanyang Business School, Nanyang Technological University, Singapore. He can be reached at *shaun.wang@ntu.edu.sg*

ENDNOTES

1 Gartner, 2017. Gartner Predicts Information Security Spending To Reach $93 Billion In 2018, Reported by Forbes. *https://www.forbes.com/sites/tonybradley/2017/08/17/gartner-predicts-information-security-spending-to-reach-93-billion-in-2018/#22a572db3e7f*

2 Gordon, Lawrence A. and Martin P. Loeb, 2002. "The Economics of Cybersecurity Investment". ACM Transactions on Information System Security, 5, 438–457.

3 Tanaka, H., Matsuura, K., Sudoh, O. 2005. Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy* 24 (2005) 37–59

4 Wang, Shaun, 2017. Knowledge Set of Attack Surface and Cybersecurity Rating for Firms in a Supply Chain (November 3, 2017). Available at SSRN: *https://ssrn.com/abstract=3064533*

5 Wang, Shaun, 2000. "A Class of Distortion Operators for Pricing Financial and Insurance Risks." *Journal of Risk and Insurance*, 67 (2000 March): 15–36.

ERM in Five Words

Part 2: Alignment, Adaptability and Resilience

By Dave Ingram

Editor's note: "ERM in Five Words" is a series of two articles. Part 1: Resilience, Transparency and Discipline was previously published in the December issue of Risk Management.

In Part 1, we talked about how Transparency and Discipline make ERM strong. But a strong ERM program is not always best for an organization. We hear stories of such ERM programs clashing with business managers and sometimes winning those fights. You only want that to happen if said strong ERM program is aligned with corporate goals and strategies. Otherwise the "wins" for ERM could be "losses" for the company.

In addition, a strong ERM program can also be brittle, meaning that it fails under unanticipated stress. To avoid brittleness, ERM must be adaptable as well. In Part 2, we address two more of the five words for ERM—Alignment and Adaptability—and how all four lead to Resilience.

ALIGNMENT

Risk has traditionally played a minor role in the strategic discussions that firms face.

Often, planners get risk out of the way at the very start with a discussion of strengths, weaknesses, opportunities, and threats (SWOT). Then, as quickly as possible, the planners shift into concentrating on a discussion of opportunities. That is what they are there for anyway—opportunities.

Risk management has been a part of business practices for thousands of years. ERM is a new approach to risk management that, when taken to extremes, may noticeably increase the cost of doing business and can take the attention of executives away from running their firms. But, through the alignment of ERM with your business plans, ERM can more than cover those costs with its benefits.

The alignment of enterprise risk management and business strategy takes place at two levels: first as part of the aforementioned strategy and planning discussion, and second, in the more operational discussions that result from the strategy and plan.

Risk Appetite and Strategy

The idea that aligning risk management and strategy is highly important may be a stretch for some businesses; but for insurers, risk is the raw material of the business. So it seems very natural that a discussion of risk management should fit well within the strategic discussion of the insurance business.

The main building block of the strategic discussion of risk and risk management is the risk appetite statement. Risk appetite is defined in the *U.S. National Association Insurance Commissioners (NAIC) Own Risk and Solvency Assessment (ORSA) Guidance Manual* as:

> Documents the overall principles that a company follows with respect to risk taking, given its business strategy, financial soundness objectives and capital resources. Often stated in qualitative terms, a risk appetite defines how an organization weighs strategic decisions and communicates its strategy to key stakeholders with respect to risk taking. It is designed to enhance management's ability to make informed and effective business decisions while keeping risk exposures within acceptable boundaries.

ERM Tools

Besides risk appetite there are several ERM tools that can aid in the strategic risk discussion.

Risk Profile

A part of the statement of the impact that the plan will have on the company should be a before-and-after risk profile. This will show how the plan either grows or diversifies the firm's larger risks. Risk cannot be fully described by any single number; therefore, there is no one single pie chart that is *the* risk profile of the firm.

The risk profile should be presented so that it articulates the key aspects of risk that are the consequences of the plan—intended or otherwise. This may mean showing:

- the geographic risk profile,
- the product-by-product risk profile,
- the risk profile by distribution system,
- or, the risk profile by risk type.

By looking at these different risk profiles, the planners will naturally be drawn to the strengths and weaknesses of the risk aspects of the plan. They will see the facets of risk that are growing rapidly and consequently require extra attention from a control perspective.

And even if there are none of those reactions, the exposure to the risk information will eventually lead to a better understanding of risk and a drift toward more risk aware planning.

Risk Management View of Gains and Losses

Planning usually starts with a review of recent experience. The risk managers prepare a review of the prior year describing the experiences for each risk in terms of the exceedance probability from the risk models. This can lead to a discussion of model calibration, and possibly to either better credibility for the risk model, or a different calibration that can be more credible.

Risk Controls Review

Each risk is operated within a control system. The review of recent experience should discuss whether the control systems worked as expected or not.

Risk-Adjusted Pricing

The review of gains and losses can also be done as a review of the risk margins compared to the risks for each major business or product or risk type. Comparison to a neutral index could be considered as well. With this review, the question of whether the returns of the firm were a result of taking more risk or from better selection, and management of the risks taken, should be addressed.

Management groups may be much more interested in one or more of these tools. The risk manager must search for the approach to discussing risk that fits management's interests in order for risk to become a part of planning and strategy. Without that match, any discussions of risk that take place to satisfy regulatory or rating agency pressures will be largely perfunctory.

Recent studies[1] have found that insurers who link ERM to strategy are much happier with their ERM program. Over half of insurers who responded to a recent poll on risk appetite said that a linkage between ERM and strategy was an explicit objective included in their risk appetite statement.

Risk Tolerance and Company Plans

Risk tolerance is the term of art for the aggregate risk plan. A company can skip having an aggregate risk plan, but if they have one, that plan is the risk tolerance. So, it is probable that more companies actually have a risk tolerance and simply do not realize it.

A majority of companies who recognize that they have a risk tolerance[2] have set it to reflect the consideration of rating agency and regulatory requirements, and sometimes also include a statement about the amount of surplus that is at risk under pre-determined circumstances. So, if the insurers who do not use the term "risk tolerance" indeed have a target for their RBC ratio or for their AM Best BCAR score, they are thereby setting an aggregate risk plan, which means that they do actually have a risk tolerance.

Strategy and Plans Impact on Risk Management

ERM should stand out of the way of the aggregation of risks the insurer plans to exploit.

An enterprise risk management program will also work to align the management of individual risks to strategy and plans. At the highest level, there are four possible strategies for controlling individual risks:

- Exploit
- Manage
- Minimize
- Avoid

The company strategy identifies the risks that are going to be exploited and managed. The ERM program should be active to assure that risk management is not serving as the business prevention function for those risks.

ERM should stand aside of the aggregation of the risks that the insurer plans to exploit, and it should make sure that due care is taken with the risks that require managing. But, that care should be of the "not too hot" and "not too cold" variety that allows for the business's success.

The ERM program should also provide assistance with the processes and procedures needed to minimize and avoid the risks that are not a direct part of the insurer's success formula. Ultimately, this means plans for risk acceptance, limits and mitigation need to be carefully reviewed by ERM for each and every of the firm's important risks.

Without a Link to Strategy

If risk management is well developed into a strong, effective, disciplined, function there are two possible outcomes: it can either help achieve the business strategic objectives, or, it can be a strong force that will, at times, prevent the achievement of strategic objectives that are perceived to be too risky (see Figure 1).

An ERM program with transparency and discipline is a powerful tool for management to use. Such a program, if set on the path of alignment, can be counted on to stay on that path and to continually support the overarching strategy while providing evidence of that alignment for all to see.

Figure 1
Effectiveness of Risk Management Impacts Alignment with Strategy

Effectiveness of Risk Management	Alignment between Risk Management and Strategy: Less	Alignment between Risk Management and Strategy: More
More	Risk management works to prevent actions taken to support strategic objectives; **causing major management clashes.**	**Risk Management seen as strategic partner;** can successfully discourage actions that nave potential to stymie strategic objectives.
Less	Risk management will ineffectively oppose actions taken to support strategic objectives; **as a result, it is ultimately ignored.**	Risk management will discourage actions that it thinks may hinder strategic objectives; **sidelined from strategic discussions.**

ADAPTABILITY

Deliberately cultivating adaptability is how enterprise risk management works to reduce exposure to and losses from surprises. Here are four ways that ERM programs work to encourage adaptability.

Revisiting Risk Identification

All ERM programs start with risk identification. A company will identify its top risks—those that are a potential threat to the existence of the firm—in the initial risk identification process.

But that risk identification and prioritization process becomes less and less accurate as time passes. Depending on the areas where a company does business, it may need to revisit its risk identification and prioritization process every other year; some companies even find it easier to just repeat the process annually.

But there is a danger with repeating the process too often. If there are no noticeable changes in the risks identified or priorities from year to year, then the process that merely reaffirms the prior choices will appear to be a needless piece of excess bureaucracy.

One way to enliven the update process is to consider what others in the industry are thinking. (See 2017's Most Dangerous Risks[3]) The result you should expect is a shifting in the prioritization of risks from year to year. But it needs to be a shift of priorities that have enough credibility to actually shift the amount of thought, resources and attention towards the risks that have increased in priority. That means a shift that top management really believes in.

Emerging Risks

Standard risk management deals with "presenting" risks—the risks that we are generally aware of mostly because we have some experience or have seen others experience losses from those risks. But, we have also been warned of black swans and unknown unknowns that might come out of nowhere and knock us for a major loss. In ERM, we call those unexpected risks emerging risks. ERM includes processes for identifying and preparing for the next emerging risks.

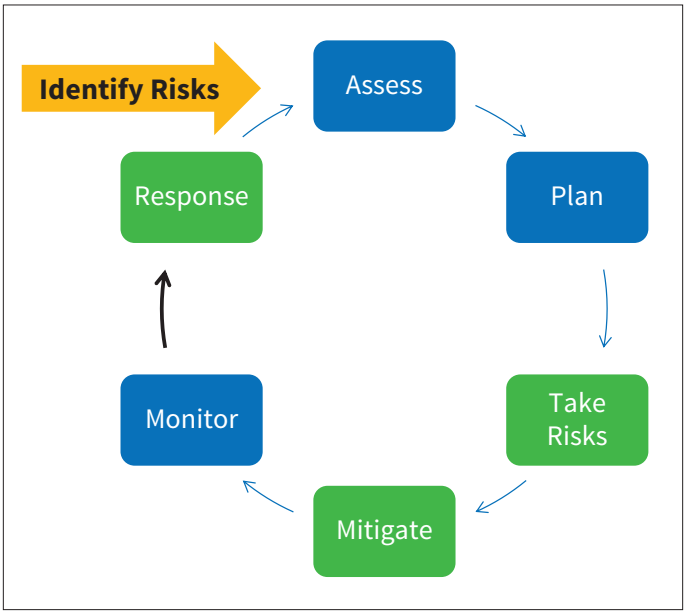
As the risk register is updated, risk managers and company executives should consider whether it is time to elevate an emerging risk into the list of important presenting risks. In the "2017 Most Dangerous Risks" survey, for example, cyber-crime made the top of the list. Several years ago, cyber-crime would have been considered an emerging risk.

Risk Control Cycle

Much of ERM takes place within a risk control cycle (see Figure 2). The risk control cycle has seven steps:

- Identify
- Assess
- Plan
- Take Risks
- Mitigate
- Monitor
- Response

Figure 2
Risk Control Cycle



Of the seven steps, the last step, Response, is the opportunity to adapt if the deviation from the plan is great enough. In a highly developed risk control cycle, the Response step will also be planned in advance.

When the situation actually occurs where the Response is needed, the actual choice might or might not be the planned Response. But companies have found that if they have discussed and planned a potential Response in advance, they can be faster in developing an actual effective Response when the need arises.

Another key feature of a risk control cycle is that it is repeated and at each repetition the Assessment step is redone. When the Assessment step is repeated, the company has the opportunity to improve the risk management process. This is especially important for a new ERM system that is best developed by a step-by-step trial-and-error process.

Risk-Learning Process

In addition to the continuous improvement that comes with the risk control cycle, companies should include a deliberate risk-learning process as a part of their ERM program. One firm made risk-learning a regular part of their risk committee meetings. The first fifteen minutes of each meeting is taken up by a risk management lesson brought to the group by a member on a rotating basis.

ERM will not be successful for the long run as a fixed, static system because risk in the real world is constantly changing, and usually in such ways that will gradually render old ERM processes ineffective. That is not a failure of those who build ERM systems; it is simply part of the nature of risk.

Continuous Improvement of Risk Management

After the initial development project ends, ERM needs to be on a course of continuous improvement. Just as the risk prioritizations of an organization are constantly adapting, the effectiveness of risk selection and mitigation processes are also evolving all of the time. Revisiting risk identification and the emerging risks process work to adapt the subject of ERM—the risks—to the present and near-term future.

The risk control cycle is designed as a feedback loop that will bring the effectiveness of last year's risk management into next year's planning. Risk learning is the part of ERM that works to incorporate lessons from both the company's own experience and the experiences of others into the knowledge bank of the firm. Adaptability is encouraged and institutionalized via ERM.

The ERM process that draws its power from Transparency and Discipline and its direction from Alignment, but only with Adaptability can ERM maintain its effectiveness over the long term.

RESILIENCE

Which brings us back to Resilience. And here we are not just talking about Resilience in the context of business continuity and disaster recovery, we are using the term Resilience in the broadest possible sense. This Resilience is the capability for an organization to survive any possible adversity and to continue operating.

With this sort of Resilience, an insurer will be able change, renew and reorganize to survive in a world and market that is constantly changing, renewing and reorganizing as well. This is where the two-sided definition of Risk becomes one again—the up side and the downside management are one and the same. In the event of an extremely adverse scenario, a vision of a new opportunity can be the ultimate form of risk management of the situation. This is adaptability.

And when an insurer has a clear vision of a new opportunity, if risk management is not aligned with the efforts to achieve success and avoid failure while pursuing that opportunity, it will be brushed aside, relegated to the periphery. However, when risk management is aligned with the new strategy of the insurer, then the discipline and transparency that make risk management strong will be eagerly accepted.

Risk management that does not adapt will not be aligned and will fight against changes in company strategies that are vital to long-term survival. Meanwhile, Transparency and Discipline are what makes ERM strong and reliable so that the organization will be able to maintain its desired strategy in many stressful situations.

Enterprise risk management is **Transparency**, it is **Discipline**, it is **Alignment** and it is **Adaptability**. Which together, all leads to **Resilience**. These five words are ERM. ■

Dave Ingram, FSA, MAAA, CERA, is executive vice president at Willis Re. He can be reached at *dave.ingram@willistowerswatson.com*.

ENDNOTES

1 *https://www.towerswatson.com/en/Press/2015/04/global-insurers-embrace-risk-management-as-a-strategic-business-partner*

2 *http://blog.willis.com/2015/04/risk-appetite-and-tolerance/*

3 *https://blog.willis.com/2017/01/2017-most-dangerous-risks-for-insurers/*

Recent Publications in Risk Management

As an ongoing feature in *Risk Management*, we will provide recent publications we find noteworthy to our readers. Please send suggestions for other publications you find worth reading to *dschraub@soa.org*, or *cheryl.by.liu@FWD.com*.

Consultation on Revising the ICP 8, ICP 15 and ICP 16
IAA
https://www.iaisweb.org/page/consultations/current-consultations/revision-icps-8-15-and-16/

Enhancing the Role of Insurance in Cyber Risk Management
OECD
http://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf

2017 Insurance CRO Survey
Ernst & Young
http://www.ey.com/Publication/vwLUAssets/ey-insurance-cro-survey-2017/$FILE/ey-insurance-cro-survey-2017.pdf

10th Survey of Emerging Risks
Joint Risk Management Section (CAS, CIA, SOA)
https://www.soa.org/Files/Research/Projects/10th-survey-emerging-risks.pdf

Big Data & Privacy: Unlocking Value for Consumers
The CRO Forum
https://www.thecroforum.org/2017/12/15/big-data-privacy-unlocking-value-for-consumers/

A Guide to Defining, Embedding and Managing Risk Culture
The CRO Forum
https://www.thecroforum.org/2017/10/06/a-guide-to-defining-embedding-and-managing-risk-culture/

SOCIETY OF ACTUARIES®

475 N. Martingale Road, Suite 600
Schaumburg, Illinois 60173
p: 847.706.3500 f: 847.706.3599
w: www.soa.org

NONPROFIT
ORGANIZATION
U.S. POSTAGE
PAID
SAINT JOSEPH, MI
PERMIT NO. 263