Southwest Audit Committee Network

June 2019

SWACN

SUMMARY of THEMES

Data privacy, risk oversight, and geopolitical risk

Members of the Southwest Audit Committee Network (SWACN) gathered on May 14, 2019, for discussions on data privacy, risk oversight, and geopolitical risk. This *Summary of Themes* synthesizes those discussions.[1] *For a list of meeting participants, please refer to page 8.*

Data privacy

Companies must balance the opportunities to capitalize on access to vast quantities of data with the potential legal, ethical, and reputational consequences that may arise from any misuse of that data. AT&T's Tom Moore and LiveRamp's Sheila Colclasure joined members to discuss approaches to board oversight of privacy practices, where four major issues emerged:

- GDPR has become the data regulation standard globally
- The US regulatory landscape continues to evolve
- Data ethics are a rising priority
- Good practices in data management are emerging

GDPR has become the data regulation standard globally

Since its implementation a year ago, the European Union's General Data Protection Regulation (GDPR) has continued to influence data regulations globally. *"It had a catalyzing effect on the world, it sets the table for everyone else,"* said Ms. Colclasure, adding that *"close to 150 countries"* now have national data laws due in part to GDPR's influence. Ongoing investigations and resultant case law surrounding enforcement continue to provide new interpretations and establish precedents. Members discussed the challenges this environment poses to overseeing compliance around the regulation. A member said, *"We worked with management and got compliant and met the deadline. What I'm concerned with is how do you keep up with all these interpretations?"* Ms. Colclasure recommended that audit committees have management conduct a periodic *"GDPR refresh"* to review the firm's current positions against the most recent case law and guidance. She added, *"GDPR is an ongoing obligation and is still evolving primarily because of regulator guidance and case law … you need to keep up with it."* Mr. Moore echoed this sentiment, noting, *"A GDPR refresh is the best practice without a doubt. I would also talk to your internal audit teams about doing a GDPR compliance check, that's a good way to have another independent yet internal body take another look."*

The US regulatory landscape continues to evolve

Ms. Colclasure noted that although the United States has been slow to adopt broad data privacy regulations on a national level, the country is no stranger to regulating data, highlighting the Health Insurance Portability and Accountability Act (HIPAA) and the Fair Credit Reporting Act (FCRA) as examples of current federal data protection laws. *"So, we are actually regulating data here and it is more rigorously enforced than anywhere else in the world,"* she added. The California Consumer Privacy Act (CCPA), set to become effective on January 1, 2020, is likely to play a major role in setting a national privacy standard. Though some details of the regulation may be amended before implementation, Ms. Colclasure said, *"about 20 states have introduced CCPA look-similar standards in the form of state legislation. That trend will continue in 2020, with some likely to pass into law."*

Data ethics are a rising priority

Consumer views regarding data privacy continue to evolve globally, as does the policy landscape. At the same time, companies must find ways to leverage their data to accelerate business opportunities or risk losing out to competitors who do.

In order to address this challenge, Ms. Colclasure suggested establishing a firm-wide data ethics framework that governs data use across the organization, adding, *"Compliance with the law is just the starting point, you need to continually look at your data practice to see if you are potentially causing harm and if the impact and consequence of the data use is fair."* She said she also expects the emergence of data review boards over the next 12 to 18 months, similar to those used in clinical trials by pharmaceutical companies. Both guests emphasized that integration of privacy concerns should not be an afterthought addressed late in the product development process. Including such features at the end of the process could lead to unforeseen issues. *"Thinking about privacy at the inception of the product or service is essential to managing the risk,"* said Mr. Moore.

Good practices in data management are emerging

Leveraging data while respecting privacy requires a sophisticated, centralized effort that draws on a range of functions inside the company. Though approaches to data collection and use vary, both guests highlighted the importance of the tone at the top when it comes to data privacy. Mr. Moore asked, *"Does the CEO think of this as a strategic imperative or a nuisance? … This is a strategic issue and it goes beyond being compliant with the legal framework."* Ms. Colclasure added, *"If the CEO thinks this is just a nuisance, this sets the tone from the top, thus the enterprise is more likely to inadvertently use data in a way that may violate a social norm or cultural norm, which will have a brand impact."* Beyond the CEO, Mr. Moore opined on the right profile of a Chief Privacy Officer (CPO), saying, *"If I'm a board member, I want a CPO who is credentialed and technically strong, but also consumer and ethically focused."* Further, both guests noted that the CPO and Chief Information Security Officer should work together

closely. *"I have a weekly call with our CISO. We are making sure we are joined at the hip in terms of our understanding,"* said Mr. Moore.

To ensure proper accountability regarding organizational uses of data, high-level decision making is essential. Mr. Moore said, *"Those processes need to be in place and have a high enough level of review so that someone with decision-making authority and accountability is reviewing it. 'I didn't know what was going on' is not an acceptable answer in accounting and it's not in data privacy."*

Risk oversight

Members were joined by John Rielly, chief financial officer of Hess Corporation, John Rogula, managing director of advisory risk transformation services for EY, and Kate Kraycirik, director of enterprise risk management for MD Anderson, to explore ways to improve board risk oversight. While ERM is relatively mature in members' organizations, questions remain about how to enhance and improve board oversight. The discussion identified practices that could lead to more robust ERM programs.

Developing a risk culture

"If you look back at the biggest risk issues and failures historically, it's almost always a culture issue," said one member. Establishing a culture of risk awareness and transparency and systematically engaging the entire organization—from the board and senior executives through the front line—is critical to risk management. The tone at the top, particularly from the CEO, is vital to cultivating the right environment. A member said, *"Risk oversight is not a difficult thing to introduce into the boardroom when the conversation starts from the presumption that this is a very important aspect of the strategy of the company."* Ms. Kraycirik explained that MD Anderson is in the process of developing an ERM program, the first of its kind for the organization, and is focused on driving the initiative into the culture of the organization. *"We asked every single employee about what the top risks were. It's really important to have the frontline people bought into this,"* she said. She shared practices her team is employing, such as enlisting every employee across the organization to aid in the risk identification process and meeting with employees to discuss the importance of the initiative.

Mr. Rielly explained how Hess has developed its ERM program and has embedded it into the company's culture: *"It is now part of our operational rhythm and just part of how we do business … but it takes a long time to set up."* Part of having a good organizational risk culture is encouraging transparency around potential issues, Mr. Rielly explained, *"We will always try to do our best, but we'll never be perfect. Compliance issues go to the board and we're not going to sugar coat it … If you can't have that discussion or your board doesn't want to hear the big problems, it's an enormous risk to your organization."* Members agreed and noted that the alignment of culture and risk has developed as board oversight has matured in recent years. *"It's a cultural issue and boards are keenly aware of that these days. That's evolutionary*

though, I think years ago boards really didn't talk much about risk but now it's a big focus," said a member.

Monitoring key risks and mitigation plans

Typically, management will make assessments regarding key risks and establish mitigation plans, which are then presented to the board. Members said it is critical to ensure key risks are regularly addressed at the board level. A member said, *"We get a sheet at every board meeting that lists the major risks and whether they're improving or declining and any related updates."* Another member noted, *"If there is a big update or change to a key risk, we discuss it as part of the operational review and will decide if we need to move capital or take other action."* Some members noted that boards should make efforts to review key risks by going beyond the management function, *"If we have a question about a specific risk, management supports and empowers us to go talk to people on the ground dealing with it."*

Beyond monitoring the key risks, it is also necessary to assess management's mitigation plans for those risks, members said. One member added, *"You need to look to make sure those mitigation plans are well thought out and that the mitigation actions are being taken, otherwise it's just a mental exercise."* A member said this is an area where internal audit can play a role: *"The value I see out of ERM is the action list of mitigation of the key risks. The other aspect is accountability: who the owner of the risk is. We're having internal audit go and visit each risk owner and confirm with them that they are doing the actual mitigation process as planned."* Sometimes boards may deem it necessary to get a third-party assessment around mitigation plans and processes for a key risk. Mr. Rielly said this could be beneficial to the organization: *"We went through that with the board. They said we see it, we understand it, [and] we want an independent review of that. This is a big risk for the company, and this is a big risk for us. A third-party came in and looked at our plans and processes and then they went out into the field to make sure our people were really following it, and we learned things from that."*

Once key risks are identified and assessed, Mr. Rogula added that a good practice for boards is to request risk quantification and monitoring to better understand organizational exposure: *"Management identifies risks and reports on mitigation strategies, but the board is rarely provided with the risk exposure. As a board member, you're tasked with understanding the exposure from the key risks, both at the individual risk level and the overall risk portfolio level, in the context of the firm's strategy."*

Allocating responsibility for key risks

Members discussed the importance of allocating clear responsibility for key risks both on the board and management levels. Mr. Rielly encouraged a collaborative environment between management and boards as they allocate responsibility: *"Once we go through the risk identification process, we take all those risks and figure out how to present to the board. Which committee does each risk belong to or does it go to full board?"* One member said, *"Each major risk that makes it to a discussion at the board level should be assigned to a*

committee or the full board, but there should also be a senior member of management attached to each of those risks, monitoring it and constantly assessing." Members also discussed the practice of having an operating committee for overseeing risks, made up of members of senior management who meet regularly. Mr. Rielly said Hess utilizes such a practice, adding, *"They all know they're responsible for the individual risks in their areas, but we have to work together to make sure we are thinking of this broadly and can handle all the risks."*

Though some members shared that their firms have Chief Risk Officers, several stressed the importance of ensuring risk management responsibility is shared across the organization. *"The CRO is really just the coordinator of ERM and shaping the program. They can't own it alone."* A few members shared concerns that having a CRO can lead to complacency, with one saying, *"I've heard of some organizations not having a CRO because then you think they're just handling risk management themselves. True risk management happens when the entire organization takes ownership of it."* Another added, *"The board is the CRO."*

Using ERM to drive strategy

In describing what a successful ERM program looks like, one member said, *"It's thorough, it's owned operationally, [and] management takes it seriously and thinks about it strategically to best allocate resources and drive the strategy of the company."* Members and guests stressed the importance of tying ERM efforts to the company's strategy. *"It's so important to drive through that ERM is not just about risk, it's also about informing opportunities and organizational strategy,"* said Ms. Kraycirik. Another member suggested the practice of mapping key risks to the company strategy: *"I asked management how our critical risks tie to the strategic plan. Because of that prodding, they now literally map the key risks to the strategic plan, and that is what is provided to the board. It sounds easy and common, but until they actually mapped it, they weren't able to see what was falling through the cracks, and they found gaps."*

Mr. Rogula suggested that boards should use ERM discussions not only to provide insights to risks of strategic execution, but also to challenge the viability of the strategy in the broader external environment: *"What are external factors that can challenge the long-term plan? You should seek the identification of risks specifically from an external perspective, to make sure the firm is considering the risks in the context of the viability of the strategy."*

Geopolitical risk

DJ Peterson, president of Longview Global Advisors, and Scott Sarazen, deputy leader of EY's Geostrategic Business Group, joined members for a discussion on the geopolitical climate and associated risks.

China

In describing the current climate between the United States and China, Mr. Peterson compared it to the post-World War II environment, saying, *"The Soviet Union went from vanquished and exhausted ally to global competitor. It was also an era of massive technological change with rockets, nuclear technology, and computers."* He added that cybersecurity will continue to play a growing role, *"My question is do we get to a Cuban Missile Crisis situation? My opinion is it will be in cyber. There were no rules at the time around nuclear weapons … my opinion is that a similar situation would be most likely to happen in cyber where those rules also do not yet exist."*

Mr. Peterson noted that the current environment has changed the rhetoric among specialists with regard to operating in China: *"Something different happening right now is the specialist community is changing their views, which is exactly what happened in the Cold War. For decades everyone has said you must be in China to succeed … it's always just been about dollars and cents, but now it's getting more colorful."* The heightened tensions between the two countries can place companies in a difficult position, said Mr. Peterson, *"In this environment as a company you can do something that makes perfect economic sense and is perfectly legal but a politician can swoop in and say 'What are you doing with China?' And put you in a very difficult position reputationally. It's become a political process."*

As the situation with China continues to develop, members discussed the viability of shifting supply chains to different low-cost markets in the region, with one saying, *"We're finding very appealing economics in other parts of the region, we are moving some operations away from China."* Mr. Peterson said, *"The issue is first, China has the scale and, second, the people, talent—no one else in the region has it … you also need to ask how much latitude those countries really have? Can China just strong arm them?"* He added, *"China is still a must-have market, the question isn't whether you will still do business, it's how."*

Mexico

Members and guests explored the developing environment in Mexico. President Andrés Manuel López Obrador, who took office in December, has taken a nationalistic approach to energy in the early days of his presidency, cancelling energy auctions for oil and natural gas projects, limiting crude imports, and halting pipeline projects.[2] In March, the administration announced plans to go forward with an $8 billion refinery as it ramps up efforts to cut back on gasoline and diesel imports coming from the United States. Mr. Peterson said, *"There is a net negative scenario emerging … the administration has become very disorganized and there is less clarity."* Members discussed political relations with the country, noting the difficulties of evaluating such a tumultuous situation. *"It's become closer to a Latin American country where it's harder to tell where you stand and where things are going,"* said Mr. Peterson.

Management practices are adapting

Mr. Peterson suggested boards should be asking a few key questions as they monitor the geopolitical landscape: *"What is your source of information? What does your management team think of the environment and where things are heading? Does the company have the ability to change course if things develop differently than expected?"* A member agreed, stressing the importance of having the right expertise in regions that are strategically significant: *"You really need boots on the ground in the region. You need people you can trust and people that understand the complexities of your business model and the market."* Another added, *"If you invested heavily in a country where there is geo risk, you should address it in every single board meeting."*

Mr. Sarazen highlighted that boards should plan for geopolitical uncertainty to be *"the new normal."* As companies develop more comprehensive approaches to evaluating geopolitical risk, Mr. Sarazen suggested geopolitical issues should be more regularly elevated to the board level, *"The best companies have processes in place to make these evaluations and get them to their boards. You need the right receptors in place, the right communications, and the ability to pivot strategy."*

Meeting participants

- John Carrig, WPX Energy
- Rodney Chase, Hess
- Marcela Donadio, Marathon Oil
- Barbara Duganier, Buckeye Partners and MRC Global
- Rodney Eads, NOW, Inc.
- John Gallagher, Kraton Corporation
- Sue Gove, Tailored Brands
- Steve Johnson, Torchmark
- Don Kendall, SolarCity
- Gil Marmol, Foot Locker
- Peter Ragauss, Williams Companies
- Don Robillard, Helmrich & Payne
- Dunia Shive, Trinity Industries
- Mike Stoltz, Windstream Holdings
- Valerie Williams, DTE Energy
- Billie Williamson, Cushman & Wakefield

EY was represented by the following:

- Randy Cain, Vice Chair and Southwest Region Managing Partner
- Scott Hefner, Southwest Region Managing Partner of Markets and Accounts
- David Pond, Principal, Southwest Region Business Development Leader
- Bill Strait, Houston Office Managing Partner

Endnotes

[1] *Summary of Themes* reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Italicized quotations reflect comments made in connection with the meeting by network members and other meeting participants.

[2] Sergio Chapa, "Mexico's new president takes nationalist tone during first 100 days in office," *The Houston Chronicle*, March 21, 2019.