Southeast Audit Committee Network

October 2019

SEACN

SUMMARY of THEMES

Fraud detection and data privacy

Members of the Southeast Audit Committee Network (SEACN) met in Atlanta on October 7, 2019. The meeting began with a visit to EY's Atlanta wavespace™ for demonstrations of fraud detection and proactive compliance management technologies. In a separate session, members were joined by guests to discuss data privacy. This *Summary of Themes* provides a brief overview of the meeting.[1]

New forensic tools to identify fraudulent behavior

At the EY wavespace™ in Atlanta, an EY team led by Virginia Adams, Jeremy Osinski, and Scott Jarrell demonstrated new tools designed to gather and filter disparate sources of data in order to identify legal, regulatory and compliance risks related to fraud and ethical conduct. By collecting and analyzing large quantities of both structured and unstructured data, companies can spot patterns and outliers for further investigation. Using cloud-based technologies such as EY Virtual, this analysis has the potential to identify the schemes that employees and third parties use to commit bad behavior and the actors who participate in them. SEACN members were shown three examples of methods that leading companies are implementing to identify and combat fraud.

In one demonstration from the retail sector, investigators combined video, facial recognition, and point-of-sale data to look for instances where employees entered "post-void" and similar transactions to pocket cash from customers rather than putting it into the cash register. Not only was the tool able to confirm the theft, but based on data trends, it found that employees were far more likely to steal cash or products in the last 30 minutes of their shifts.

Another case came from a financial institution's trading desk: the compliance function analyzed sales orders and confirmations, the quantity of trades and time elapsed, voicemails, text messages, chat terminals, and the emails of traders or sales agents to detect unusual patterns that might warrant deeper investigation.

The third demonstration focused on identifying anomalous patterns in travel and entertainment expense reimbursement requests, customer sales visits, and speaker programs in the pharmaceutical and life sciences industry. As sales practices in that industry are heavily regulated, outlier expenses can be an indicator of unlawful activity. This particular tool was able to consolidate siloed information from various platforms into a single hub and make connections that would not otherwise be apparent.

These demonstrations offered examples of how companies are deploying advanced analytics to create a more dynamic approach to fraud risk. Members raised questions, however, about what might prompt a company to invest in these capabilities and whether and how companies might take a phased approach to adopting these tools. For example, one participant asked about starting with analyzing existing data before expanding data collection methods.

The risks and challenges of data privacy

Companies must balance opportunities to capitalize on vast quantities of data with the legal and reputational consequences of misusing it. As companies explore new ways to gather and use data, these risks will become increasingly relevant to board discussions about strategy and risk. Tom Moore, chief privacy officer (CPO) at AT&T, and John Mason, chief information officer (CIO) at Quorum Health, joined members to discuss these challenges.

- **New privacy laws have been a catalyst for change.** New legal requirements have caused many companies to enhance their approach to privacy oversight. In particular, AT&T's Mr. Moore noted that the European Union's General Data Protection Regulation (GDPR), which he described as the de facto global standard, *"ushered in a broader concept of privacy,"* and *"requires a deep program of data protection officers, document retention policies, training, assessment, and compliance organizations that didn't previously exist."* Due to the sweeping nature of GDPR and the substantial consequences for violating it, many companies have designed their privacy programs to be GDPR compliant in all jurisdictions. Mr. Moore cautioned, however, that as state-level requirements like the new California Consumer Privacy Act (CCPA) are developed and implemented across the United States, there will be instances where legal requirements conflict, making compliance even more confusing and costly. Quorum Health's Mr. Mason noted that while privacy has been an imperative in the healthcare sector for decades, *"some deeper pushes to monitor, track, and protect information"* have come as a result of the Affordable Care Act and new privacy laws. Over the past few years, he noted, there has been a distinct *"shift to a more activist role [with] regulators proactively looking for potential privacy violations."*
- **Reputation risk is a key consideration.** Historically, privacy was treated as a compliance and security risk. Members and guests discussed how that is changing. Even explicit consent from customers and employees to use data in a manner fully compliant with regulations is not always enough. It is difficult for firms to anticipate public perception of any new or unusual use of data, particularly because what people say about their views on privacy does not always align with their actions, e.g., their willingness to trade personal information for convenience. Both guests noted that privacy risks also extend beyond an information security breach. Mr. Mason said, *"Security is the process that tech puts in place to secure your castle; the most critical information sits at the core. Privacy is more about what you are doing to ensure that data is not shared beyond its appropriate use."*

Despite the risks, new uses of data enhance its value to companies and their ability to use It effectively can add value to customers. That needs to be communicated effectively. Mr. Mason stressed that properly channeled data use can lead to breakthrough innovations: *"Health care companies use data to improve outcomes. We need to tell a better story about the beneficial uses of data while making sure we keep it private."* Mr. Moore added, *"The future is personalization, but it is impossible to personalize products and experiences without data*," and doing so is *"paramount to the long-term success of a firm."* Yet, Mr. Mason cautioned that in some cases, the consequences of misusing data are so high that companies must consider whether the potential benefits outweigh the risk. For example, he advised members to consider monetizing data only *"if it's core to your mission,"* given public sensitivities to such uses.

- **Principles like "privacy by design" can help companies strike a balance.** As a consequence of both new regulations and reputational concerns, privacy is now being considered earlier in the product or service development process. Mr. Moore described the concept of privacy by design: *"You build privacy into new products or services from the beginning. You don't bolt it on later."* He added that for new products, AT&T conducts a *"privacy impact assessment, like an environmental impact assessment. When we develop a product, we assess the data we propose to collect, how long we'll keep it, how we'll use it. We have to know that it'll be not only compliant with the law or our privacy policy but good for the brand."* Mr. Moore acknowledged, however, that doing this effectively is much more challenging for older companies with legacy systems not designed for privacy considerations than for newer tech companies with more advanced data management capabilities. Members suggested that being transparent with employees and with customers about how their data is being used is essential.
- **Oversight of third-party relationships is a growing concern.** Privacy becomes an even more complicated issue when companies share data with third parties. Mr. Mason said, *"In healthcare, we have to watch that a lab or software company involved in your treatment doesn't use your data in different ways. They may de-identify, but you have to make sure it's de-identified enough; you'd be shocked at [how] much you can re-identify."* He added, *"We can't do business with a third party without a business associate agreement. They have to be willing to be held fully accountable at the same level as we are. We just won't do business with companies that don't have adequate procedures in place."* Mr. Moore said that in some cases it takes six months before AT&T will do business with a vendor, and only after a thorough process that might include sending AT&T's information security professionals out to audit the vendor's practices. Boards should understand company policies and controls related to data sharing with third parties.
- **Management structures for privacy oversight vary dramatically.** Firms are still working out how to best structure privacy oversight. Given the growing importance of this issue, cross-functional collaboration is critical to success. How companies treat data and privacy

"depends on size, and where this issue falls within the risk profile," an audit chair said. Not every firm needs a CPO, but all companies need to think about how functions like IT, compliance, risk management, legal, and human resources engage with one another on these issues. Mr. Moore emphasized that *"every discipline needs to be represented at the table,"* and agreed with members that *"the first line of defense is the business."* He added, *"I suggest you also get your internal audit team to check how your company is doing in this area."* Mr. Mason said that as CIO, he and the chief compliance officer work together closely on the issue, often in collaboration with the chief information security officer and the general counsel.

- **Privacy is becoming a focus for boards**. At some companies, privacy is now a regular item on board or audit committee agendas and at others it is just starting to receive board-level attention. For many SEACN members' companies, advanced uses of data and their related privacy risks are not yet getting significant board-level attention. A member observed, *"What strikes me is how much the business you are in affects where this sits on the risk profile."* Mr. Mason and Mr. Moore presented examples of more mature models for privacy management and board oversight. Mr. Moore said that he presents to AT&T's audit committee and public policy committee on a regular basis, noting that in the past 18 months privacy topics have been discussed with the board or one if its committees six times. He added that to make those sessions most effective, *"I come with metrics: How many requests are we getting from consumers or employees? I discuss our readiness for CCPA; hits we've gotten in the media."* Mr. Mason also works very closely with the board, though he noted that privacy is just a piece of his broader conversations about information technology and information security.

Meeting participants

- Eddie Adair, Rayonier Advanced Materials
- Denise Dickins, Watsco
- Juan Figuereo, PVH
- Andre Hawaux, Pulte Group
- Tom Hough, Equifax
- Jim Hunt, Brown & Brown
- Rich Macchia, Fleetcor
- Rick Mills, Commercial Metals Company
- Maureen Morrison, ePlus and Safeguard Scientifics Inc.
- Jason Papastavrou, United Rentals
- Terry Rappuhn, Akorn, Inc.
- Alice Schroeder, Quorum Health (Northeast Audit Committee Network member)
- Bill Smith, Southern Company
- David Walker, Chico's FAS, CommVault Systems, and CoreLogic
- Rick Williams, Crawford

EY was represented by:

- Cigdem Oktem, Director, Southeast Region, Center for Board Matters
- Dave Sewell, Audit Leader, U.S. Central Region, Partner
- Bryan Yokley, Georgia/Alabama/Tennessee Market Segment Leader, Assurance Partner

Endnotes

[1] Summary of Themes reflects the network's use of a modified version of the Chatham House Rule whereby names of members and their company affiliations are a matter of public record, but comments made before and during meetings are not attributed to individuals or corporations. Guests, however, have given permission for their remarks to be attributed. Comments by guests and network members are shown in italics.