Northeast Audit Committee Network

June 2018

NEACN

SUMMARY of THEMES

Third-party risk, cyber breach response and disclosure, and the blockchain

The opportunities and risks resulting from new technologies were an underlying theme when members of the Northeast Audit Committee Network (NEACN) met on June 5, 2018 to discuss third-party risk, cyber breach response and disclosure, and the blockchain. For a full list of meeting participants, please see page 6.

Third-party relationships increase risk

Large companies engage a wide-range of third parties that can number into the thousands, depending on the company and industry. These relationships are increasingly complex, global, and a significant source of organizational risk. Members explored the board's oversight of third-party risk with Jim Connell, head of third-party oversight at JPMorgan Chase, and Corliss Montesi, vice president and corporate controller at Stanley Black & Decker.

The discussion started with Mr. Connell and Ms. Montesi sharing how their organizations approach third-party risk management. At JPMorgan Chase, Mr. Connell has a centralized team of 300 people who oversee the third-party risk policy, manage regulatory engagement, onboard new third parties, and conduct supplier assessment processes. Centralization allows a consistent approach to supplier assessment and third-party performance audits and provides a single repository of information for internal and regulatory reporting purposes. Stanley Black & Decker operates more of a hybrid model, with supplier management and IT maintaining centralized processes including risk scoring and *"sacrosanct"* criteria that suppliers must adhere to for onboarding.

Members then discussed the operational, reputational, and cyber risks they see associated with managing third-party relationships. At JPMorgan Chase, Mr. Connell said the *"top risk is cybersecurity... Operational risk is second place."* While cybersecurity is critical everywhere, Ms. Montesi said that Stanley Black & Decker also thinks of third-party risk in terms of *"what it could mean for disruption to the business."* Issues relating to procuring products and accessing and maintaining distribution channels are critical.

Whether a centralized or decentralized process, members expressed concern about "one-offs" where people don't follow the established protocols for onboarding new third parties to the company. Mr. Connell said, *"We're extremely vigilant about people not going through the process. We've gone through a reconciliation process and found 10 or 20 suppliers that were on-boarded without going through the process in the past few years. If we catch someone, we*

make a spectacle out of it." To mitigate this risk, Ms. Montesi explained that Stanley Black & Decker utilizes "*internal audit to look at the contracts to see if there were circumstances where they didn't go through the process."* JPMorgan Chase has also teamed up with four other banks to set up a company, TruSight, to execute shared supplier assessments using agreed upon industry standards. TruSight allows JPMorgan Chase to improve third-party oversight, manage risk, streamline its processes, and reduce costs. Although specifically geared to financial institutions, members agreed that TruSight has potential in other industries. A member said, *"TruSight was very interesting. It raises the question: 'Is there a way to do this more efficiently and effectively?'"*

Third-party risk often falls under the audit committee's purview as part of the risk oversight process, according to members. Certain third-party situations may be escalated to the full board due to their material nature or unique circumstances, such as relating to cybersecurity. In providing members with some parting thoughts to help shape their discussions with management, Ms. Montesi advised, *"From a very basic level, do you have standard processes for assessing third-party risk and where are they standard? How do you get comfortable with management of that risk? What are the other things that tend to trip you up, those things outside of the norm?"*

Lessons from a cyber breach

Joe Corbett, CFO of the United States Postal Service (USPS), and Seth Berman, a partner at Nutter McClennen & Fish, joined members to discuss the USPS's cyber breach and the key points learned from that and other recent breaches.

- **Expect to grapple with uncertainty.** Companies need to be prepared for an extended period of uncomfortable uncertainty in the early days of an attack. Mr. Berman said it may be unclear whether there has been a breach, how widespread the breach may be, and whether the hacker is still active in the system. It may take days or weeks to investigate, determine how and why the breach occurred, and assess its implications. For example, Mr. Berman described one case where *"someone offered to sell a client information that they found on the web. It ultimately turned out it was the result of an external hacker. However, the client was several steps behind in the process, as they kept looking only for the insider they believed leaked the materials. Whenever a breach occurs, it is important to ask, 'Is this the tip of the iceberg or the iceberg itself?'"*
- **Communication is critical but challenging.** Uncertainty creates internal and external communication challenges. Once Mr. Corbett learned of the USPS breach, the Audit Committee Chair and Chairman of the Board were immediately notified. An internal team was then formed under a project management office and this team communicated initially via an outside network every day. According to Mr. Berman, "*What is really hard to accept as an executive at a company that has been attacked is that you feel like you are the victim of a crime. However, the reality from a PR perspective is that most people outside the*

company will view the company not as a victim, but as the cause the breach, since the company failed to protect their data. From their perspective, you are the perpetrator, not the victim. This mismatch in perception often leads to regrettable public statements from management." Boards need to be mindful of new regulatory activity intended to impact cyber breach disclosures, including the SEC's new cyber disclosure guidance, which requires boards to disclose their role in overseeing cybersecurity, and the EU's General Data Protection Regulation (GDPR), which mandates that communication of a breach take place within 72 hours of an attack.

- **Bring in outside experts.** When breached, engage outside forensics experts and the General Counsel's Office because these situations will likely end up in litigation. Getting the right individuals engaged early is critical because according to Mr. Berman, **"***These types of crises bring out the worst in people. What seems totally obvious as the next steps to one senior executive are not obvious to everyone else around the table who may see things quite differently. This can result in an internal power struggle that slows or even impedes the response."*
- **Shift the focus to prevention, detection, and remediation.** Once the crisis formally passes, management must act. USPS made significant investments in people, processes, and infrastructure. Mr. Corbett recommends setting up cyber teams at very senior levels within the organization, testing, reviewing system entitlements, implementing dual authentication, benchmarking, and, above all, having a plan in place for next time.
- **The board must get actively involved.** Knowing the plan for handling a cyber attack and participating in scenario planning are ways that boards can engage with management on cybersecurity. As Mr. Berman said, *"The most important takeaway is that the board must have a more active role than in the past. You should aim for the same level of oversight of cyber security that you have over financial controls. If you move in that direction, you'll stay ahead of the SEC, and put yourself in the best position in case of other litigation. From a prevention perspective, boards must move from beyond the sidelines. Spend some time and money figuring out where you are and what you can learn from past problems."* The message resonated with members. One remarked, "*You need a plan. As a board member, you have to go in there and really demand it."*

De-mystifying the blockchain

In 2017, venture capitalists invested over $1 billion in blockchain technology. But blockchain remains a bit of a mystery. EY Partners Mark Kronforst and Scott Zimmerman joined members to explain the technology, discuss potential applications, and explore regulatory and audit issues for blockchain and cryptocurrencies.

Mr. Zimmerman described blockchain as a new technology to manage an old problem: transaction processing. There are three interesting characteristics of this technology. First,

the ledger of all transactions is distributed among all blockchain participants. Each participant has a complete copy of the ledger, which makes any tampering of the ledger self-evident. Second, the ledger is programmable, which means that the ledger can store both the details of transactions and the logic describing business processes that should follow or govern each transaction. The third notable characteristic is that adding transactions to the ledger, or blockchain, requires a consensus agreement among the participants that the new set of transactions are accurate and complete. Again, this makes it practically impossible to manipulate a large blockchain.

Mr. Zimmerman described several practical applications for the technology. Cryptocurrencies, such as Bitcoin, are the most prevalent blockchain application today. Blockchain technology is particularly useful in connecting large numbers of organizations and establishing a shared set of facts and business processes. As an example, he described a blockchain application in the shipping industry where insurance rates are determined in part by where the cargo has passed through and how long it remained in that area. Blockchain would enable insurers to calculate premiums quickly and accurately as compared to the current complex and time-consuming process. While blockchain applications are starting to emerge, the technology is still in its infancy and there are significant implementation and regulatory challenges to be overcome to permit its mass commercialization. One member commented, "*I thought we were much further along. We are still in the very early stages and I'm really not that far behind.*"

Mr. Kronforst said auditors are already beginning to engage with blockchain technology. He said that audits involving blockchain will include reliance on work performed by specialists and traditional audit procedures. Specialists in programming and cryptography will be needed to understand, in part, *"what is this supposed to do and is it functioning that way?"* As the technology becomes more ubiquitous, regulators will become more engaged. Mr. Kronforst noted that regulators are already struggling with a number of issues related to cryptocurrencies including:

- **Jurisdictional issues (Who regulates what?).** A cryptocurrency can qualify as a security under the federal securities laws and be subject to robust regulation by the Securities and Exchange Commission.
- **Balancing innovation and investor protection.** Regulators must balance facilitating new ways to form capital with ensuring that investors are adequately protected.
- **Valuation.** Cryptocurrencies that are widely-traded such as Bitcoin present fewer challenges than those that are more thinly traded.

About this document

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.

Meeting participants

The following Northeast Audit Committee Network members attended all or part of the meeting:

- Bert Alfonso, Eastman Chemical Company
- Carl Berquist, Beacon Roofing Supply
- Pat Gross, Waste Management
- Lew Kramer, L3 Technologies, Inc.
- Gracia Martore, WestRock
- Maureen O'Connell, Sucampo
- Terry O'Donnell, ePLus
- Craig Omtvedt, General Cable and Oshkosh
- Craig Owens, The J.C. Penney Company & Dean Foods Company
- Marianne Parrs, Stanley Black and Decker
- Mike Ranger, Covanta
- Ron Waters, Fortune Brands Home and Security

The following Northeast Audit Committee alumni members attended:

- Jay Morse, Alumnus

EY was represented by the following:

- Mark Besca, New York Area Office Managing Partner
- Rich Jeanneret, Americas Vice Chair
- Kevin Virostek, Greater Washington Managing Partner