CENTRAL
AUDIT COMMITTEE NETWORK

Summary of Themes

October 19, 2017

TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781 290 2270

Audit chairs discuss tax reform, information security, and activist investing

Board members are confronting a number of challenges as they attempt to steer their companies through uncertain waters. Members of the Central Audit Committee Network (Central ACN) convened in Chicago on October 3, 2017, to discuss tax reform, the information security function and chief information security officer (CISO) role, and new trends in shareholder activism. Members were joined by James Holley, CISO of Caterpillar, and Robbie Higgins, CISO and Vice President of Enterprise IT Risk at AbbVie, for a session on the board's oversight of information security. Over dinner, Phil Denning, a Partner at ICR, spoke about lessons learned in crisis communication, with an emphasis on shareholder activism. In addition, Gary Gasper, Co-Leader of EY's Washington Council, joined members for a discussion on impending tax reform.[1] For a full list of meeting participants, please see page 6.

Tax details emerge for companies to use in scenario planning

Following the release of a high-level outline of the Republican tax plan, members discussed timing and how tax reform was likely to proceed. Mr. Gasper noted the administration needed to provide an outline of its tax plan to ensure it would have sufficient support to get a budget resolution bill approved by the House (subsequently approved on October 5, including a special procedures provision that will allow the Senate to approve a new tax bill by a simple majority). It is expected that the tax proposal would reduce the corporate tax rate from 35% to 20% and apply a first-time minimum tax rate of between 10%–15% to foreign earnings. In addition, companies would be provided an opportunity to repatriate earnings, most likely at a split rate for liquid and illiquid assets.

Members raised concerns about which deductions may be discontinued as part of tax reform. Mr. Gasper said various trade-offs will be necessary to get the bill passed by both the House and Senate, and he anticipated a best-case scenario of a House vote by Thanksgiving, a Senate vote in early December, White House approval shortly thereafter, and a new tax law in place by the end of 2017. He said, *"There is sufficient detail now available so that companies can model different scenarios to determine potential implications. Wall Street analysts will likely be interested to hear about tax and earnings impacts during upcoming 3Q17 or 4Q17 earnings calls."*

Boards wrestle with information security oversight as challenges evolve

Facing a threat that is both evolving and existential in nature, audit committees and boards are taking a closer look at the information security function, its leader, and its role within the broader organization. Companies and boards are mindful of the importance of protecting critical data and assets both today and in the future. Several key themes emerged from the conversation in Chicago.

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

Summary of Themes

Prioritizing security investments is critical to effectiveness

Both Mr. Holley and Mr. Higgins acknowledged that it is impossible to secure every aspect of a business, so boards and management teams need to prioritize the most critical data and systems. Mr. Higgins said, *"You've got to know what is critical to the business and what may affect it. For us, intellectual property, trade secrets, and patient data is the critical sensitive data."* Mr. Holley agreed and told members his team asks the business to provide a net present value calculation for sensitive collections of information and uses that value to establish security criteria: *"If business leaders tell me it has high value, I'll put differential protections around it and put it in the high-value vault."* He also noted, *"Businesses understand that they don't want to put everything in the vault because, while it's much more secure, it's also more difficult to share data in the vault with third parties who may need it to provide a service to us. So we're very selective about what goes in there."* In setting security priorities, one member stressed, *"I don't think you can overemphasize understanding management's view of what the 'crown jewels' are."*

In addition to being capable technology leaders, CISOs must also be knowledgeable about the business and how it will evolve. Mr. Higgins has an internal security advisory board made up of senior business leaders to help him identify risks and priorities for the business and for information security going forward, while Mr. Holley gets similar input directly from executive officers on a more informal basis. Mergers and acquisitions, timely application of software patches, and retiring old equipment that falls short of security protocols (e.g., USB drives, iPads, etc.) were identified as known risks that must be dealt with. Mr. Higgins said, *"Inevitably bad things will happen – any CISO who says otherwise, I would be highly skeptical of. So the critical question becomes, how do you identify quickly, limit your exposure, and recover fast?"*

Placing a cyber discussion in the business context helps board communication

Members and guests stressed the importance of direct communication between the information security organization and the audit committee and/or board. Mr. Holley noted, *"When I brief the audit committee … they have to be comfortable and confident that we have people, process, and technology in place to find intruders and kick them out before they can accomplish their goals."* Both guests said they provided briefings a few times a year to the audit committee and that information security would be on the audit committee's agenda more frequently if necessary. Several members reported a similar reporting cadence, while others said that they received more frequent reporting or that the reporting on information security went to the full board. One member reported that the Chief Information Officer (CIO) attends every board meeting to provide an update on information security, while another said that the CISO is on call to answer questions every time the audit committee meets.

Mr. Holley and Mr. Higgins identified commonalities in their reporting approaches: avoiding technical reports in favor of stories that illustrate both the risks and the maturity of the security profile, aligning their reporting with business priorities, and framing their reports to the board in business terms. Mr. Holley said, *"I have to help the audit committee and board understand our risks in plain business terms. The board doesn't need a technical discussion, but a business discussion. If I can't do that, we need a different CISO."* Mr. Higgins said, *"[It is] incumbent on me, the CIO, and the leadership team to put reporting in business terms that makes sense to the board."*

Common frameworks, like those developed by the National Institute for Standards and Technologies (NIST) and the International Standards Organization (ISO), are used by information security officers as a basis to measure the progress of their program toward maturity and frame their reporting to the board. Mr. Holley said, *"What the board needs to know is that the leadership understands the risks, what our current posture is, that we have set risk-based goals, have a plan to achieve those goals, and our progress toward those goals."* Commenting on a reporting framework he uses, Mr. Holley described a process involving *"measuring maturity in multiple information security domains, setting maturity targets, and reporting to the audit committee on how we are achieving progress in those domains. We have set goals and made investments in getting to our target maturity state."* One member recalled asking questions such as *"Is the target along the line to maturity high enough, and what are you doing to get there from where we are?"* Another member noted the value of *"picking a framework that's appropriate and then thinking about maturity as opposed to compliance. What's the destination, and where are you on the journey?"*

Making cybersecurity everyone's job has a strong impact

Mr. Holley and Mr. Higgins agreed on the importance of engaging employees in strengthening their firms' security profiles. For instance, Mr. Higgins described a capability that has been integrated into his firm's email system to engage employees by allowing them to flag potential phishing emails with a single click: *"If you get a suspicious email, you click a button and it's forwarded to information security … We used to get a few dozen suspicious emails sent to us; but, since we deployed the click button in 2016, we've gotten over 86,000 identified by end users, which we can now automatically review and block where appropriate."*

Third-party risk must be addressed and reported to the board

Both members and CISO guests emphasized that giving third parties access to sensitive data carries security risks. Boards must be sure that potential suppliers or partners have the necessary security systems in place. Mr. Higgins noted that he focuses on third parties in his reporting to the board. His business depends on *"lots of third parties [so] now we have to figure out how to share critical data and control and secure it."* One member said, *"Third parties are a fact of life. In our business we need a host of third parties. The audit committee can insist that there is a process for looking at suppliers to ensure their security systems are equivalent to what they should be – you go and establish security specs that they have to meet."*

Boards find assurance in third party assessments of information security

Members and guests emphasized the value they see in third-party security assessments. One member noted, *"A core principle for us is we are going to have a third party to come in and give us a punch list [of security concerns]."* Another member reported that they had *"a vendor we were using for third-party security monitoring to give us comfort, and it was a positive to have them doing the work for us because they see so many more of the viruses hitting companies."* Mr. Higgins said that his firm periodically brings in outside organizations to benchmark and conduct reviews and assessments, including an overall annual assessment and periodic penetration tests. Mr. Holley said that, *"I have our organization tested 30 to 40 times a year by one of eight different companies. I don't rely on an annual test to say we are secure … We say [to the third-party firm], go find what you can find."*

Challenges posed by activist investors

Mr. Denning noted that recently activist investors have been taking on larger companies, targeting CEOs for operational issues, and looking at companies undergoing CEO transition. He said there have been more attacks from investors with short positions and that activist investors are using media outlets more. These trends appear to be driven by the activist investment cycle and changes in media coverage as well as by the activists' revenue model, which requires them to increase returns as well as assets under management so they can grow fees.

According to Mr. Denning, *"Activists in the past looked at multi-business companies, then financial engineering, and are now focused on agitating for operational changes, where they have to come in with a detailed analysis of the business and competitive environment. This is the trend in the activist cycle.*" Members agreed that directors nominated by activists these days are far more qualified than those nominated in the past. In line with what can be seen as a maturing activist cycle, Mr. Denning highlighted the emergence of a dedicated media beat on activism, with journalists at major outlets seeking a constant stream of content on shareholder activism and looking to activist investors for stories and ideas. This in turn helps smaller activist funds attract attention and, consequently, assets.

The increase in attacks by those taking short positions in stocks was of particular concern for members. Mr. Denning referred to *The Capitol Forum,* an online research publication, which appears to have a relationship with short sellers. Mr. Denning reported that his firm had identified a *"correlation between short campaigns and coverage in* The Capitol Forum. *The short thesis gets out there in* The Capitol Forum *research, which is frequently cited in short reports."*[2] A guest CISO who joined members for dinner added, *"Cyber is the next short frontier,"* and shared the example of a cybersecurity company that suffered a short attack after some of its customers were hacked.

These trends make it more important than ever to engage in *"planning in peacetime,"* according to Mr. Denning. He suggested measures such as an *"investor perception audit"* – asking a third party to evaluate how investors perceive the company and identify what potential weaknesses an investor might exploit. Mr. Denning also noted the importance of communication to investors: *"In peacetime you get credit for outreach, so disclose it; say how many investors you reached out to."* A member endorsed this suggestion, saying, *"You have to bring in your advisers annually to assess your vulnerabilities … [You need to] have a good idea of how to respond [to questions such as] why the company is not buying more stock, not splitting up, etc. If you don't know how to answer these questions, you will be on the defensive."*

[2] Further information can be found in the attached memorandum from ICR.

Summary of Themes

About this document

The Central Audit Committee Network is a select group of audit committee chairs from leading companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is organized and led by Tapestry Networks with the support of EY as part of its continuing commitment to board effectiveness and good governance.

Summary of Themes is produced by Tapestry Networks to stimulate timely, substantive board discussions about the choices confronting audit committee members, management, and their advisers as they endeavor to fulfill their respective responsibilities to the investing public. The ultimate value of *Summary of Themes* lies in its power to help all constituencies develop their own informed points of view on these important issues. Those who receive *Summary of Themes* are encouraged to share it with others in their own networks. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.

Summary of Themes

Meeting participants

The following members attended all or part of the meeting:

- Anne Arvia, GATX
- Howard Carver, Assurant
- Sandy Helton, Principal Financial Group
- John Holland, Cooper Tire & Rubber Company
- Clay Jones, Cardinal Health
- Blythe McGarvie, LKQ
- Mike Merriman, Invacare and Nordson
- Bob Murley, Apollo Education Group
- Neil Novich, Beacon Roofing Supply
- Sherry Smith, Deere & Company
- Ingrid Stafford, Wintrust
- Steve Strobel, Newell Brands

EY was represented by:

- Richard Bonahoom, Partner, Business Development Leader, Central Region
- Robert Braico, Partner and Advisory Account Leader for United Health Group