SOUTHEAST
AUDIT COMMITTEE NETWORK
VantagePoint

February 1, 2008

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

Information technology governance

Introduction

The Southeast Audit Committee Network held its ninth meeting on January 15, 2008, to discuss the audit committee's role in information technology (IT) governance. This document is a synthesis of insights and comments from the meeting. In an extensive private session, members also discussed the wide-ranging impact of the subprime lending crisis, with a particular focus on its impact on corporate liquidity and capital markets.

During the meeting, members discussed the following topics:

- **Information technology risks and opportunities**
- **Addressing the challenges of IT**
- **Immediate action boards can take**

Collectively, members of the network in attendance at the September meeting sit on the boards of more than two dozen large-, mid-, and small-cap public companies. Audit committee chairs attending were:

- Denny Beresford, Kimberly-Clark and Legg Mason
- Kerm Campbell, SPX Corporation
- Renée Hornbaker, Eastman Chemical Company
- Doug Ivester, SunTrust Banks
- Claude Lilly, FairPoint Communications
- Dean O'Hare, Fluor Corporation and H. J. Heinz Company
- Tom Presby, World Fuel Services, Invesco, and Tiffany & Company
- Jim Robbins, DSW
- Erik van der Kaay, RF Micro Devices
- Bunny Winter, Wellesley College

Also attending the meeting from Ernst & Young were:

- Edwin Bennett, Southeast Area AABS Managing Partner
- Tom Hough, Vice Chairman and Southeast Area Managing Partner

VantagePoint 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 during the meetings are not attributed to individuals or corporations. Members' remarks appear in italicized quotes.

Executive summary

Information technology allows corporations to realize explosive growth and high returns, but it brings with it substantial risks and potential pitfalls. Board directors must understand the growing, critical role that IT plays in their companies in order for them to provide the appropriate level of oversight.

- **Information technology brings risks as well as opportunities** *(Page 2)*

  As one member noted regarding IT, *"There are always new risks – a couple hundred a year!"* Audit chairs say that during board discussions of information technology, directors need to keep a careful eye on three major areas: data theft and cyberterrorism, failures in IT leadership, and risks related to mergers and acquisitions. As with many areas of the business, *"it's not just the questions you ask, but how you verify the answers you're given."*

- **How do we equip ourselves to address the challenges of IT?** *(Page 4)*

  The IT challenges facing companies are plentiful, but so are the options for addressing them. Members discussed the possibility of forming a separate technology committee, but recognize that merely forming a committee does not solve the problem of obtaining much needed IT expertise. By increasing technological expertise on the board and turning to external sources for guidance, directors can gain more comfort with how IT is being managed. An extensive list of questions for board directors to consider as they pursue various IT governance objectives can be found in the appendix on page 7.

- **Boards can take some steps immediately** *(Page 5)*

  There are a number of actions that directors can take right away to get a better understanding of how IT is managed. Many of these actions involve building relationships with the CIO and IT department and experiencing the technology firsthand. Getting started early is important, given that when it comes to IT projects, *"fits and starts can cost a company hundreds of millions of dollars."*

Information technology brings risks as well as opportunities

Technological improvements often bring both new opportunities and new risks, and that has certainly been the case with information technology. As one member noted regarding IT, *"There are always new risks – a couple hundred a year,"* and robust oversight of the IT function is critical for avoiding or managing an IT-related crisis. As defined by Ken Doughty and Frank Grieco, information technology governance is a "framework that supports the effective and efficient management of information resources (e.g., people, funding, and information) to facilitate the achievement of corporate objectives. The focus is on the measurement and management of IT performance to ensure that the risks and costs associated with IT are appropriately controlled."[1] In our discussion, members identified three major areas of IT risk that they face: data theft and cyberterrorism, IT leadership failures, and risks related to mergers and acquisitions.

[1] See Ken Doughty and Frank Grieco, "IT Governance: Pass or Fail?" *Information Systems Control Journal* 2, 2005. Available at http://www.isaca.org/Template.cfm?Section=JOnline&CONTENTID=24195&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

The risk to information security

One risk all corporations face is the loss or theft of data – either customer data or intellectual property. Members discussed the difficulty in balancing the need to be able to exchange information freely with the need to *"manage intellectual property risk"* and not have critical information just *"floating around."* One member remarked, *"The ability to control data in a collaborative environment is challenging."* Another member agreed and expressed frustration over the fact that *"too many people [have] access to some applications, and not the right people [have] access to others."*

A data breach can result in long-lasting reputational damage in the marketplace, as demonstrated by the 2007 theft of data from TJX Companies.[2] And breaches are becoming more common: the Identity Theft Resource Center stated that "more than 79 million records were reported compromised in the United States through December 18 [2007]. That is a nearly fourfold increase from the nearly 20 million records reported in 2006."[3]

The impact of data theft reaches far beyond the specific loss and the cost of closing the breach. One member shared that *"there was an act of data theft around the time of our initial public offering. It's hard to get around the issue. It stung with the financial community and with the Federal Trade Commission."* For companies in industries that might be the target of hostile attacks, *"cyberterrorism is an issue of enterprise risk,"* one member said. *"If the wrong person gets access to the network, they can cause a disaster. The IT department is focused quite a bit on that."* Other members expressed similar concerns around access to their systems and networks: *"our auditor sat in our parking lot and cracked our wireless network in minutes. They got past the perimeter, and we were under the impression that we were secure."*

Addressing failures in IT leadership

A number of members shared stories of failures in IT leadership – in some cases, multiple failures in a very short period of time. One member described going through multiple CIOs. The CIOs appeared to the board to be great candidates. The member involved said that lack of IT expertise on the board had prevented the directors from recognizing that the candidates were not appropriate prior to their being hired. *"This question is at the heart of Enron and other tragedies,"* one member remarked. The member noted that as a board director, *"it's not just the questions you ask, but how you verify the answers you're given."*

Another member, who had faced a similar situation, said, *"We went through a drill and asked, 'Do we have the capabilities and backgrounds on the audit committee to challenge the CIO?' It reminds me of the 1970s and 1980s, when the audit committee members had no requisite [financial] experience. [We need to have] the right people with the right skill sets."* Many members agreed, with one noting that *"it would be easier for most of us to spot a bad CFO than a bad CIO. That probably reflects our bias or training."*

---

[2] In February 2007, the theft of credit and debit card information from TJX Companies put at risk the credit and debit information of customers who shopped at TJX Companies stores (such as TJ Maxx and Marshalls) from 2003 through December 2006. The number of affected customers has exceeded 45 million.

[3] Associated Press, "Personal data loss hit record level in '07" *Boston Globe*, December 31, 2007. Available at http://www.boston.com/business/articles/2007/12/31/personal_data_loss_hit_record_level_in_07/.

Technology concerns during mergers and acquisitions

Companies experiencing rapid growth through mergers and acquisitions often feel the pain of trying to integrate multiple technology platforms after a deal is complete. *"Our company is acquisitive; we've done scores of acquisitions over the years,"* one member said. *"As long as we're in that mode, [IT issues] are first and foremost in our minds."*

How do we equip ourselves to address the challenges of IT?

The IT challenges facing companies are plentiful, and as members indicated, so are the options for addressing them whether through forming a special committee of the board, increasing the number of directors with technology expertise, or using external resources.

Form a special committee

While all public boards have committees that specifically address the finances and board governance, most directors find that IT issues are tacked onto a committee that has a primary focus on other issues – often the audit committee because of its interest in the technology behind internal controls and its oversight of risk management. Some companies are recognizing the need to form separate technology committees to focus on IT governance. One member serves on a board in which *"IT was addressed by a subcommittee of the audit committee and then was broken out"* to be a separate, stand-alone committee of the board to provide time for more in-depth discussion of IT issues.

However, members cautioned that simply developing a separate technology committee is not a panacea for IT issues. As one director noted, *"Having a separate committee doesn't [address] the competency of the directors"* serving on it. The committee needs members with some relevant expertise if it is to be useful, although the precise type of expertise is unclear. Does a former CEO who managed a CIO have the requisite experience? After all, a former CEO is regarded as a financial expert if they managed the CFO.

Increase technology expertise on the board

Improving the oversight of IT often starts with an attempt to bring new knowledge and experience to the board. *"It's a basic governance question,"* one member remarked. *"Do you have the skills on the board to assign [to] committees? You need to recruit board directors like you do employees – skills based. I'm going to go back to the governance committee to review how we select our next directors and ask if they will have [IT expertise]."*

Having one board director who is a technology expert may not be enough, and overreliance on one person's IT knowledge may be more problematic than having no experts at all. One member who serves on the audit committee of a technology company noted, *"All of our directors have run small or large organizations [that have dealt with] IT development."* Even so, the member acknowledged that *"we can't staff [up the board] enough to protect us from every issue we might face."*

Another member described how a board recruited a prominent business school faculty member with deep technological expertise: *"He's a one-man IT committee who everyone respects."* One audit committee

chair noted that the benefit to recruiting academics is that *"in theory, [they] want to be right on top of what is going on"* and might have knowledge of emerging best practices. However, as another member pointed out, *"people like that are rare."*

In addition to bringing in directors with IT experience, companies can also try to increase the level of knowledge among the directors they already have. Directors typically have the opportunity to attend sessions and courses as a component of their director education. However, although there are a large number of IT-related sessions directors can attend, one member confided being afraid *"[I] wouldn't understand the course [content]."*

Look outside the company for guidance

When a board cannot immediately acquire expertise, they often go outside the company for advice and guidance. One audit committee chair said that *"an outside firm was brought in to advise us and help us understand what 'best in class' was and what were the right processes to manage IT to its maximum ability."*

Another had done the same: *"The audit committee hired a consultancy. The board discussed it, and the audit committee was quite vocal. We consider IT to be a customer service group, and [internal] users were asked about them anonymously. We asked our customers to rate us, too. When you consider that [a customer depends on us], bad IT [on our end] could shut them down. They come in and evaluate us, too, and we're also evaluated by our external auditor."*

Additionally, several members praised the guidance that their external auditor provided: *"They've been very good at getting us focused."* Members also noted that *"the external auditor can bring in experienced people."* Even if the lead audit partner does not have IT experience, he or she can call on others in the firm for assistance.

Boards can take some steps immediately

In addition to the longer-term solutions that companies can put in place to provide better oversight of IT, members highlighted several near-term actions they could take to get a better handle on IT matters. Two of the three suggestions – have regular board or committee meetings with the CIO present and spend time in the function and with the people – involve relationship building and seeing things firsthand.

Have regular board or committee meetings with the CIO present

Although members agreed on the value of regular contact with the CIO, the length and frequency of these interactions varied widely. One member said, *"I walk around [the IT function] and talk with the CIO. Not that I know what to look for! It's a far cry from saying I'm accomplishing anything, but it's something, and it shows I'm interested in them and what they're doing."*

Some members reported having *"a one-on-one with the CIO yearly,"* while others reported meeting with them *"quarterly"* or more often. The relationship between the CIO and the audit committee chair allows each to gain a deeper understanding of what the other is interested in and working on. When it comes time

for the CIO to meet with the audit committee, *"the CIO gets to point out what he's doing [that we're interested in], and we don't [complain] about his budget."*

As for CIO meetings with the full board or audit committee, practices vary depending on the specific situation of the company. One board has *"an annual review with the CIO at the full board,"* while another meets with him *"quarterly."* For many boards, the frequency of interactions *"depends on what is going on [in the company]. We meet once a year with probing questions. We discuss IT as it relates to corporate strategy and effectiveness."* Another company had *"annual reports to the audit committee from the CIO"* until they undertook a major company-wide IT project. *"It was so huge, we want quarterly reports from the CIO for two years, until the system is functioning."* This is a common practice with major IT projects, given that *"fits and starts can cost a company hundreds of millions of dollars."*

Spend time in the function and with the people

"It's important to talk to others in IT [beyond the CIO]," one member commented. *"Drill several levels down to the people doing the actual work."* Several members agreed, and one suggested *"talking to the end users about their involvement with IT and their concerns"* as one way to get a better view of the function. While members broadly agreed with this point, one audit chair argued that *"you're a director – how many hours can you spend [digging around]?"*

Use internal audit to conduct specific IT-related audits

One member receives *"regular reporting from internal audit on the IT function. The quality of IT internal audit has increased over the last few years."* This audit chair also *"talks to the heads [of both IT and internal audit] about how they view each other's functions."* Another member shared, *"We direct internal audit's scope development, and in the risk assessment, some IT issues will come up, and we figure out how to address them [during the audit]."*

Conclusion

As the economy enters into a period of potential slowdown, IT spending may not increase as much as it has in the past, but even so, technology market research consultancies predict growth in spending in the 4–6% range.[4] The IT function is clearly of continuing importance. It brings with it many advantages – lower costs, new markets, added revenue – but also many risks, including failures in leadership and application and system failures. The key to successfully navigating these challenging waters rests with people: having the right directors on the board, having them organized properly, and building relationships with key individuals throughout the company.

[4] Allan Altar, "2008 IT Spending Predictions," *CIO Insights*, December 27, 2007. Available at http://blogs.cioinsight.com/research_central/content001/spending/2008_it_spending_predicitons_1.html

Appendix: Questions for boards to consider as they pursue IT governance objectives[5]

Assessing the alignment between the organization's business and IT objectives

Objectives: Reach understanding and agreement between business and IT about IT's role and its business contribution. Get senior management in both IT and the business involved and accountable for IT governance and supportive of the board in setting direction.

Key questions to ask:

- Is there clear board-level accountability for IT in your organization?
- What training does the board receive to enable effective and confident discussion of IT? How confident are board members about initiating and maintaining that IT discussion?
- Do board members understand the IT spend and its link to the business strategy and objectives? To what extent is there common understanding of what IT value means?
- Can board members articulate and agree on a set of critical IT assets and risks? Are the areas of interdependence between IT and business risks clearly identified? How confident are you that risks are being addressed consistently across the organization?

Overseeing management of IT investment to achieve value

Objectives: Evaluate proposed new initiatives, prioritize them, and monitor progress. Ensure project goals and objectives remain consistent and that expected benefits are achieved, whilst allowing for the inevitable changes in business needs and risks that arise during lengthy programs. Understand the cost drivers and issues in IT, the extent and nature of budgets and spend, and how spend is monitored.

Key questions to ask:

- Are the board, IT management, and finance in alignment about how to articulate, measure, and monitor IT costs and value?
- How is business stakeholder buy-in and accountability for new system investments and business benefits achieved?
- Is there a formal and rigorous portfolio evaluation approach for potential new projects? Is it consistent and well understood, and does it recognize the need for multiple evaluation criteria according to the specific program?

[5] Prepared by Ernst & Young following the April 3, 2007, Canadian Audit Committee Network meeting as a resource for audit committees and other board directors.

Addressing compliance requirements

Objectives: Have a framework and process that ensure compliance requirements are identified and addressed efficiently and effectively. Be confident that the IT-related controls in place will permit comprehension of and efficient compliance with the myriad of IT-related compliance requirements.

Key questions to ask:

- Are you confident that you really understand the implications of IT-dependant compliance programs such as SOX 404, MI 52-109, IFRS, and EU 8th directive?
- Do your internal and external advisers assess and report to the board on compliance with IT-related regulatory requirements?
- Is there an enterprise-wide and formal approach to ensure awareness of forthcoming compliance requirements and compliance with at least minimum requirements?
- Is there clear accountability for achieving and maintaining compliance? Are results reported to the board on a regular basis?
- How do you embed compliance in the organization once the initial work to achieve it has been completed?

Ensuring performance is measured

Objectives: Increase the likelihood that the perception and reality of IT's performance and contribution to the business will be in alignment. Have confidence that sound investment decisions are being made based on accurate and relevant information. Bring all stakeholders into agreement on what is important, and craft a framework that permits measures to be adjusted as the business evolves and success criteria change.

Key questions to ask:

- Is there an agreed-upon business view of successful IT performance? Do you have discrete measures for large strategic IT investments?
- How have you determined what to measure, and have you ensured that you have the necessary measurement tools and processes in place? Do you receive reporting on performance against these measures?
- What actions are taken as a result of IT performance measurement?
- Is the approach to measuring IT integrated with the approach and timing for measuring business performance?
- Does your measurement framework provide for changes in business priorities and therefore changes in IT performance measures?

Developing and implementing a consistent risk management framework

Objectives: Have a visible means whereby individuals can raise concerns and identify red flags. Have confidence that programs will deliver accurate reports of risks. Have clear criteria for go/no-go decisions at critical stages in the program and the ability to change or stop failing programs on a timely basis.

Key questions to ask:

- Is there a clearly articulated and well-understood risk management approach across the enterprise? Is it applied to IT?
- When did you last see a comprehensive IT risk assessment? Was it independently verified?
- How confident are you that risk assessment and management is a real core competency across the organization?
- How confident are you that a rigorous approach is taken to categorizing IT risks? Once risks have been categorized, do only the high risks get discussed?
- How do you measure the effectiveness of your risk management strategies and activities?
- Is risk management truly embedded in the organization, or is it regarded as the domain of auditors and compliance?

Developing the right IT organization and resource management

Objectives: Have formal and regular assessment of the IT organization, both to achieve value from IT expenditure and to make the right trade-offs between costs and risk when making IT sourcing strategies and decisions. Be confident that the IT organization is cost-effective, that it delivers systems at costs that are comparable with industry leaders, using well-trained and skilled staff, and that it is effective at resource balancing. Provide a structure within which resources, recruitment, compensation, and benefits can be assessed. Understand early warning signals of potential mismatch between IT capability and desired business goals. Maintain the ability to manage outsourcing arrangements.

Key questions to ask:

- How do you align your IT organization with your strategy?
- When did you last justify the numbers and balance of skills of people in your IT organization?
- When did you last carry out a rigorous organizational capability assessment of your IT organization?
- How does your IT organizational capability influence your sourcing decisions?
- How do you justify your IT training budget? Is it aligned with your IT strategy?
- How easily, and at what cost, can sourcing decisions be reversed or changed after they have been made?

Ensuring effective governance of third parties

Objectives: Clearly articulate and agree on objectives and standards from the start and support them with well-constructed contracts aligned with specific requirements. Have a governance framework that addresses the full outsourcing cycle. Ensure thorough due diligence and set key performance indicators before deals are signed.

Key questions to ask:

- Are key stakeholders agreed on the primary and secondary objectives for working with a third party? Is it to increase efficiency, cut costs, gain access to skills, or to support step change in the organization?
- Is there a good cultural fit between your organization and the potential third party? Does the third-party organization maintain similar values?
- Are there clear criteria and mechanisms to measure success?
- How confident are you that you have the skills to manage the third-party relation effectively?
- Is responsibility and accountability clearly defined, documented, and understood, both within your organization and that of the third party?
- Do you receive the appropriate level of assurance from third-party providers regarding their performance as measured by the key compliance and risk measures embedded in the agreement?

About this document

The Southeast Audit Committee Network is a select group of audit committee chairs from leading North American companies committed to improving the performance of audit committees and enhancing trust in financial markets. The network is convened by Ernst & Young and orchestrated by Tapestry Networks to access emerging best practices and share insights into issues that dominate the new audit environment.

VantagePoint 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 *VantagePoint* lies in its power to help all constituencies develop their own informed points of view on these important issues. Anyone who receives *VantagePoint* may share it with those in their own network. The more board members, members of management, and advisers who become systematically engaged in this dialogue, the more value will be created for all.