# Board Perspectives: Risk Oversight

## Briefing the Board on IT Matters

Issue 67

When directors are briefed on IT matters, do they fully understand the message? Or is the message so complex that it gets lost? Below, we discuss three contexts for conducting IT briefings with the board. Each provides directional insights for the chief information officer (CIO) and the chief information security officer (CISO) in organizing delivery of the briefing and to directors for information they should expect to receive.

In today's environment, many businesses are actually "technology businesses" because their business models cannot function without technology. Innovative technology can be a differentiator as well as a disruptor in the marketplace. Technological advancements are rapidly compressing the half-life of business models. Industries that historically have not been viewed as dependent on technology are now being transformed by it. Almost no business is immune. For example, consider London's black cabs or Uber. Online booking and the ability to track a cab, call a cab from anywhere, and manage an account from mobile devices are significant differentiators. Bottom line, technology is no longer a mere enabler.

We often receive feedback from board members stating they do not have a sufficient understanding of the IT risks facing their organizations. This feedback is sourced from roundtables we have facilitated and interactions with directors serving our clients.

According to a 2013-2014 public company governance survey conducted by the National Association of Corporate Directors in the United States, IT was the area with the least amount of satisfaction in terms of both quality and quantity of information received from management.

The board needs to understand IT as a critical enterprise asset, and the opportunities and risks associated with it must be communicated in a manner directors can understand. Directors instinctively know IT risks have increased in significance. Social business, cloud computing, mobile technologies and other developments offer significant opportunities for creating cost-effective business models and enhancing customer experiences. They also may spawn disruptive change, increased privacy and security risks, and further exposure to cyberattacks.

The fresh challenges presented by these changes create, in effect, a "moving target" for companies to manage. While the velocity of disruptive innovation through emerging technologies is not as immediate as a sudden catastrophic event, its persistence of impact is potentially lethal for organizations caught on the wrong side of the change curve.

Add to all of the above the evolving relationship between the CIO and CISO and the board of directors (or the supervisory board in a two-tiered board structure). These dynamics sum up the environment and expectations that these executives face as they address boards now and in the future, placing their interactions with the board within a business model, strategic and/or risk context.

## Key Considerations

In many organizations, the CIO and CISO brief the full board or the audit committee at least annually, if not more frequently, on the state of IT. The following are three ways they can approach this briefing:

- **Within the context of the business –** The CIO or CISO addresses how the business model leverages technology to deliver the products and services the company offers the marketplace and the opportunities and exposures resulting from disruptive change. The business context briefing answers questions such as:
  1. Do we understand the developments in potentially disruptive technology at an industry level? Are we sufficiently ahead of the change curve such that we are able to integrate new technologies into the business on a timely basis?
  2. Are emerging technologies being deployed effectively to achieve our business objectives (e.g., achieve customer loyalty, improve quality, compress time, reduce costs and risks, and drive innovation)?
  3. Are we positioning the company's operations to anticipate and proactively drive the innovative change needed to secure sustainable competitive advantage?
  4. What emerging technologies could alter the competitive landscape, customer expectations, and strategic supplier and/or distribution channel relationships within the value chain in which we operate? To what extent are our operations and the technologies we currently deploy exposed to disruptive change and being held captive to events in the foreseeable future?
  5. Are there aspects of our technological capabilities that we should be sharing with analysts, shareholders and the street, in general, in telling our story? If so, are we sharing them? If not, why not?
- **Within the context of executing the strategy –** The CIO or CISO articulates how strategic initiatives are driven by critical technologies and how the organization is facilitating the design and implementation of controls over these various technologies to ensure they perform effectively. The strategic execution context briefing answers questions such as:
  1. What technologies are critical to implementing our strategic initiatives (e.g., growth, profitability enhancement, innovation and process improvement)?
  2. How are we ensuring these technologies are functioning effectively?
  3. How are IT and the business collaborating to ensure that an appropriate return on the organization's investment in these technologies is being realized?
  4. What challenges are we encountering in implementing these technologies to execute our strategy? What is the potential impact of these challenges on the success of our strategic initiatives?
  5. Do we have the reliable and timely information and data we need to execute strategic initiatives?
- **Within the context of mitigating risks –** The CIO or CISO uses a broader business view to identify specific risks that either may be a result of technology or are mitigated partly through the application of technology. The risk mitigation context briefing answers questions such as:
  1. What are the most significant risks arising from IT, and how do they affect the business, including its reputation and brand image? Have we assessed our tolerance for these risks?
  2. Are we mitigating the critical risks to an acceptable level? How do we know?
  3. What critical business risks are we mitigating using a risk response that relies upon an important technology component? Is this technology component performing effectively? How do we know?

The objective is to provide a briefing on IT matters that resonates with directors across all of the above contexts:

1. **The business context:** Are we managing disruptive change?
2. **The strategic context:** Are we maximizing value contributed and return on investment?

3. **The risk mitigation context:** Are we managing the business and reputational impact of our risks?

Underlying the above discussion are two principles, now timeless: (1) business objectives are also IT objectives, and (2) IT risks represent business risks. Using these principles, the above contextual perspectives provide insights to CIOs as to how they should communicate with boards and to board members as to the information they should expect from CIOs.

Citing and then speaking to the above contexts in a crisp, nontechnical manner can facilitate an ongoing board dialogue. In this regard, the CIO or CISO should:

- **Demonstrate an understanding of the business –** Using the appropriate context, drill down to the relevant IT-related objectives, plans for achieving objectives, organizational capabilities to execute plans, and measures by which to gauge progress. In today's world, technology can facilitate and expedite business transformation and growth through technological innovation (the business context), but it also can destroy reputations if not adequately protected and controlled (the risk mitigation context). Board members should be counseled on both of these interrelated contexts.
- **Focus on the board's needs –** The board has little interest in the intricacies of how the CIO or CISO organization is run and managed. Don't go there unless requested.
- **Address business impact and metrics, not just IT impact and metrics –** Provide an end-to-end view and focus on business consequences. For example, consider the following metric: "99 percent of our systems are patched within 10 days." This metric leaves unaddressed the question as to the sensitivity of the data and/or business consequences of service failure of the other 1 percent of systems.
- **Target the audience –** It is important to understand the purpose of the briefing. Ask the board committee chair for direction. Ask people who have presented to the board for insight as to the background and personalities of the various directors.
- **Keep it pithy –** Directors don't want the whole nine yards. Focus on what they need to know, and leave it at that. Share sophisticated knowledge carefully. Identify the message points directors should take away, and focus on supporting those points. Allow time for questions. Expect to be asked to expedite your briefing if it is scheduled late in the day.

Boards need to clarify their expectations of the CIO and CISO. What are the directors' needs, what is it they don't understand, and what IT issues and related business risks concern them the most? More important, what context(s) do directors want these executives to address when presenting on IT matters? In addition, directors need to be realistic with their expectations of CIOs and CISOs due to the natural complexity of IT. Accordingly, the allotted presentation time should be commensurate with directors' expectations of the briefing.

## Questions for Boards

Following are some suggested questions that boards of directors may consider, based on the risks inherent in the entity's operations:

- Are opportunities presented by technology and the potential to lead and/or respond to disruptive change influencing the strategy-setting process? Or, alternatively, is technology simply viewed more narrowly as a strategic enabler?
- Does the board devote sufficient time to IT matters, including related opportunities and risks, as well as the organization's capabilities and processes in managing those opportunities and risks?
- Is the board satisfied with the CIO's periodic communications? If not, has the board conveyed its expectations to the CIO, so that future communications are on point?
- Is the CIO organization effective in supporting the changing needs of the business and monitoring technology innovations, including how new technology can be deployed by competitors (or employees) to create disruptive change? Does the CIO assist the board in understanding these issues?

- Given growth in the number of cyber threats confronting organizations, does the board have an active dialogue with the CISO on incident response preparedness?
- For significant IT projects, does the board understand the underlying assumptions about how each project achieves strategic goals, as well as how success will be measured? Is there follow-up to ensure that each significant project delivers on promises made?

## How Protiviti Can Help

Protiviti works with company executives to maximize return on information systems investments and minimize IT risks. Using strong IT governance and program management practices to ensure alignment with business strategies, Protiviti drives excellence through the IT infrastructure and into supporting applications, data analytics and security. Our comprehensive suite of IT consulting services covers three main areas of focus to help our clients leverage technology to address critical business priorities: technology strategy and operations; security and privacy solutions; and enterprise applications solutions.

## About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.nacdonline.org/Magazine/author.cfm?ItemNumber=9721. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* will be consolidated into a printed booklet that will be co-branded with NACD. Protiviti will also post these articles at **Protiviti.com.**

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®
Risk & Business Consulting.
Internal Audit.