Deloitte.

On the board's agenda | April 2016

In this issue...

Extended enterprise risk management

Understanding third-party risk

A supplier's factory collapses killing hundreds of workers, some of them children. Thousands of customers' credit card information and other personal financial records are hacked after a third-party is granted access to an organization's network. A major product recall needs to be launched when the organization discovers that a supplier used contaminated materials.

Concerns around vendor risk were once almost exclusively related to the quality of products or materials being provided or the risk that a vendor might be unable to meet delivery of supply quotas, thereby disrupting production.

Today, under the US Foreign Corrupt Practices Act, the UK Bribery Act and similar legislation in other jurisdictions, organizations are increasingly being found liable for their suppliers' behavior. Similarly, customers also don't differentiate an organization from its suppliers. They view an organization as being the provider of a solution and if a problem occurs, they hold the organization responsible and it is the organization's reputation that may suffer. Given this, organizations today should broaden their risk oversight to include the extended enterprise,[1] including third-parties' health, safety and environmental practices, compliance with labor laws and other regulatory requirements, use of intellectual property, practices around the sourcing of raw materials, corruption, and more.

One of the biggest challenges facing boards and organizations is gaining an understanding of the full extent of their third-party relationships and the associated risks.

For these reasons, third-party risk is increasingly becoming an item on board agendas. A recent Deloitte global survey of 170 organizations found that 87 percent of respondents faced a disruptive incident with third-parties in the last two to three years. The survey also found a growing acceptance of the need for enhanced accountability for third-party risk management at the board and C-suite level to ensure the explicit linkage of risk and strategy in maximizing the opportunities from their third-party ecosystem.[2]

[1] In a globalized business environment, no organization is an island. The ecosystem of a typical organization comprises an exceedingly large number of entities with which the organization does business, including customers, partners, agents, affiliates, vendors, and service providers. Taken together, these third-parties constitute "the extended enterprise."

[2] Deloitte, *Third party governance and risk management: The threats are real*, 2016

Understanding the extended enterprise

One of the biggest challenges facing boards and organizations is gaining an understanding of the full extent of their third-party relationships and the associated risks.

Large organizations, for example, with thousands of third-party relationships often lack a clear picture of their full extended enterprise. Most organizations' ecosystems include secondary or tertiary level parties, which may be entirely unknown to the organization, yet whose behavior could still have an impact on the organization and its reputation. Third-parties may also be located in different jurisdictions with different local business and cultural norms, practices, and standards—which could make oversight of them and their business practices a challenge.

Boards should ensure that the organization has determined how and where third-parties and their activities could potentially expose the organization. The organization, therefore, should develop a comprehensive view of its entire third-party risk universe that identifies where risks are concentrated in terms of suppliers, products, commodities, geographies, and other factors. In areas of extreme concentration, organizations should consider diversifying their third-party relationships.

Managing the risks

Organizations need to understand what risks in their extended enterprise could increase the level of vulnerability of the organization. Boards should ensure that management includes third-party risks in its overall risk assessment and that sufficient measures are in place at the board and C-suite level to enable the organization to manage all of the risks down its value chain, including having the appropriate counter measures in place when an issue arises with a third-party. One practice includes ensuring that the organization's insurance coverage is sufficient to protect the organization in the event of a major failure at a third-party.

Despite focusing on a wider range of vendor risks than they once did, some organizations' methods of managing third-party risk still have yet to evolve. For example, some continue to take a contract management approach to third-party risk, believing that the due diligence undertaken before a contract is signed sufficiently mitigates the ongoing risks associated with that third-party.

In these situations, no further risk assessments are undertaken and the organization adopts a reactive approach to third-party risk management with problems often being identified and addressed only after they have occurred and the damage is done.

One approach that some organizations take to manage their third-party relationships is to develop preferred supplier lists. Few organizations, however, extend that to risk-rating the third-parties on the list—identifying those whose operations have been monitored and found to be of top quality, compared to those relationships that the organization needs to more proactively manage and control, and those that the organization won't engage with at all.

To proactively manage their third-parties, organizations should identify and set out their standards and expectations around key practices to which they are expected to adhere. An organization should also include provisions in its contracts that describe the type of validation, monitoring, testing, and other assurances that the organization may require to confirm that third-parties are meeting these standards. For example, third-parties may need to provide annual confirmations of their adherence to the organization's core values, while the organization may reserve the right to visit third-party sites to undertake its own verification of the third-party's practices. Agreements with third-parties should clearly state that failing to meet the organization's standards will nullify the contract or result in performance measures.

Although many organizations have third-parties that operate in jurisdictions with different regulatory requirements, business practices, and ethical standards, the activities of third-parties are increasingly judged according to the standards of the organization's home jurisdiction. It is appropriate, therefore, that organizations push their values out to the extended enterprise, but in doing so they need to be mindful that not all of their practices may translate directly to a third-party's situation and there may be the need for some local adaptation. The existence of good two-way communication channels between the organization and the members of its extended enterprise can help ensure that the organization's standards and values are being embraced by its third-parties.

Mark Victor
Partner, Governance, Risk & Compliance
Deloitte South Africa

"One of the biggest risks an organization could face would be the lack of a full knowledge and understanding of its extended enterprise. The board needs to ensure that the organization gains this understanding by developing a complete inventory of its third-parties and overseeing the controls and processes that management puts in place to proactively manage third-parties, with the objective of mitigating risks while improving quality and reliability of the third-party relationships."

Questions for directors to ask

1. Has our organization completed a comprehensive third-party risk assessment and, if so, what are the most significant third-party risks facing the organization today?

2. What third-parties have the potential to significantly disrupt the organization's ability to achieve strategic goals and objectives?

3. What is being done to manage and proactively monitor risk as it evolves within our extended enterprise? What risk management tools do we use?

4. Who is responsible for managing third-party risk within our organization?

5. How often does management update the board on its assessment of third-party risks and the processes it has put in place to mitigate those risks? Are these updates of appropriate timeliness and level of detail?

A director's perspective

José Écio Pereira serves on the boards of directors of Votorantim Cimentos, Fibria, and Gafisa and is a past board member of BRMalls; he chairs the audit committees of Votorantim Cimentos and Gafisa. Mr. Pereira is the founder and owner of JEPereira Consultoria em Gestão de Negócios and is a retired partner of Deloitte Brazil.

Is third-party risk an item on board agendas?
The boards that I am familiar with undertake a risk assessment every three or four months, and while third-party risk isn't a specific topic on their agendas, it is part of that overall discussion of risk. That said, boards are definitely devoting more attention to third-party risk now compared to just a couple of years ago, and in Brazil that is mainly because of the Clean Company Act of 2014. Under this anti-corruption law, organizations can be found liable for illegal activities or unethical behavior of their third-party suppliers.

Because of this law, boards are looking much more closely at the risks associated with their organizations' third-party suppliers. That includes examining the suppliers' labor practices, employee standards, work conditions, health and safety measures, and other factors to ensure that all of them conform to the standards of the organization that has hired them. Another major concern, especially with the current economic situation in Brazil, is the financial health of a third-party supplier. Organizations want to be sure their suppliers are paying their taxes and meeting their legal obligations, especially as they relate to their employees, and that the supplier's business will be sustainable.

Are they looking at third-party relationships from the perspective of cyber risk?
I believe that organizations that have interconnected systems with their third-party suppliers for supply and logistical purposes are aware of cyber risk and are taking the necessary steps to manage it. But that is generally related to the flow of goods and services.

On a broader level, I would say that most organizations don't have the appropriate information systems to support them in managing their third-party relationships. Many organizations don't have systems that are sophisticated enough to connect with the systems of other organizations and, as a result, organizations use a variety of tools to manage these third-party relationships and often they are not very well integrated. For example, some organizations use multiple systems, including manual tools or spreadsheets manage these relationships, which is something these tools were never designed to do.

Who should "own" the responsibility for third-party suppliers?
The board has a role in providing oversight and ensuring that senior management has a process in place to manage third-party risks.

What we're seeing in Brazil is that the procurement department continues to be responsible for the operational issues and ensuring that the goods and services are being provided by the third-party supplier as required under the contract. In addition, many organizations are also setting up a special function to manage the contracts related to third-parties. Most Brazilian companies have several third-party relationships—for example, food services, site security, transportation, and manufacturing services—and all of these are critical to the organization's day-to-day business. So, to manage these relationships effectively, many organizations are dedicating more resources to contract management

Organizations are also monitoring their third-parties on a day-to-day basis to ensure contract compliance. Furthermore, many organizations require their third-parties to conduct self-assessments around compliance—in addition to the organization performing periodic contract audits and other tests to verify compliance. All of that is a big job, and it can take a special management function to carry it out.

Let me give you a real life example. One of the companies that I work with is building a major new facility—an investment of almost US$2 billion that will take about a year and a half to complete. At the moment, the construction process is just getting underway and there are a number of third-party suppliers contributing to the project, everything from providing site security to supplying and installing equipment.

The organization created a steering committee for the project, which includes members of its executive board. That committee meets at least once every two weeks and one of the recurring items on its agenda is the relationships with the third-party service providers. The focus is on much more than just due diligence; it also includes the ongoing monitoring of the third-party suppliers.

The steering committee provides the board with a project update on a monthly basis. That report includes any issues related to the third-party providers, such as a failure to remit employee withholdings, failure to pay municipal taxes or social security benefits, not following health and safety site rules, as well as operational issues, such as a supplier not delivering the required quality of work or being unable to meet deadlines. When problems are identified, the steering committee includes them as risks on its risk map for the project, and follow-up actions are taken by management under the terms of the contract, including the application of prescribed penalties.

Should organizations also set out their own ethical standards for their third-party suppliers?
Following the introduction of the Brazilian anti-corruption legislation, most organizations reviewed their ethical standards and codes of conduct and one of the major changes they made was to add procedures and rules that apply to third-party suppliers.

In the past, all the processes around ethical standards, including training and workshops, was undertaken from an inside perspective. It applied to people within the organization, but it didn't extend to outside service providers. Now, organizations have extended their standards to their third-party suppliers, including those related to employee standards, health and safety measures, working conditions, legal behavior, and other activities. They have also extended their training programs; most organizations require suppliers to attend seminars and workshops where the rules are discussed and the monitoring processes are explained.

In the past, all the processes around ethical standards, including training and workshops, was undertaken from an inside perspective. Now, organizations have extended their standards to their third-party suppliers, including those related to employee standards, health and safety measures, working conditions, legal behavior, and other activities.

Contacts

Dan Konigsburg
Managing Director
Global Center for Corporate Governance
Deloitte Touche Tohmatsu Limited
dkonigsburg@deloitte.com

Michael Rossen
Director
Global Center for Corporate Governance
Deloitte Touche Tohmatsu Limited
mrossen@deloitte.com

www.global.corpgov.deloitte.com

Visit our Global Center for Corporate Governance website to find relevant resources to support your board's needs.

Acknowledgements

The Deloitte Global Center for Corporate Governance would like to thank all of the professionals who assisted with drafting, editing, and reviewing this publication, including those listed below:

Co-authors: Chantal Rassart (Canada) and Hugh Miller (Hugh Miller Communications).

Technical Reviewers: Michael Rossen (United States), Timothy Scott (Canada), and Kevin Tracey (United States).