Beware weak links in the chain

Boards might be focused on the risks in their own company, but suppliers can harm their image too — and let in the cyber thieves

Carly Chynoweth Published: 7 February 2015

Promoting partnership: Don Kenny, chief executive of Lavendon

When a company's suppliers get it right, they provide good value and innovation to go with the product or service. When they get it wrong, however, they can become a source of financial and reputational damage — or even a back door for cyber criminals.

It is risk to which few boards seem to be alert, according to David Archer, a partner at Socia, the leadership organisation. "In our experience, executive directors are usually focused internally on ensuring they hit their own targets and, while some nonexecutive directors are trying to look at the whole picture, it is difficult for them to really see into the supply chain."

But with companies becoming more reliant on third parties to deliver products and services, acquiring that overview is a strategic imperative.

"Suppliers should be a board issue, not just for executives but for nonexecutive directors, too," said Rob Alexander, a partner at Occumen, the management consultancy.
"If you are not clear on the construction of your supply chain, you could get caught out by reputational issues such as suppliers breaching labour regulations. Or you could have exposure in terms of currency fluctuations and movements in commodities."

Then there is the question of cyber security. Big companies put a lot of time and effort into protecting their computer systems and the information they hold, but they could still be vulnerable if their suppliers don't do the same, said Phil Huggins, vice president at Stroz Friedberg, a risk management company. "We have seen major breaches as a result of weaknesses in the supply chain. Suppliers are drawn from many sectors, including small and medium businesses that in many cases do not have professionals dedicated to cyber security."

In some cases those weaknesses might allow criminals to gain access to data held by a third party, but in other cases the supplier might simply be a soft way in. The hackers who stole millions of customer records, including credit card information, from Target in 2013 appear to have broken into the American retailer's computers through its heating and cooling system, which could be remotely managed by the company that supplied it. The Wall Street Journal reported that the thieves stole login details from the supplier and used these to break in.

"We encourage boards to treat this [cyber security and suppliers] as one of their mainstream risks," said Jane Jenkins, a partner at Freshfields, the law firm. "They need to address the competency of their suppliers to handle their sensitive data in the same way that they would look at insolvency risks. They should not fall into the trap of thinking that it is just an IT problem — it is far more than that."

For example, they could require suppliers to cooperate in a security audit or to achieve a cybersecurity standard. They might even choose to help small suppliers build resilience into their systems, added Huggins. "And one of the key questions that nonexecutive directors should ask of executives is, 'Are you judging the relationship with suppliers based on the financial value they provide or the level of trust we place in them?'."
Archer advises nonexecutive directors to make time to visit suppliers: "We tell boards to get out more, to do 'look and see' visits, to smell and touch what is going on." He acknowledged that this sort of activity takes significant commitment and will not always be practical, but said it is worth the effort when there are big potential risks. "They [nonexecutive directors] need their eyes wide open . . . they should also look down the chain at how suppliers treat their suppliers. You can't mitigate risks unless you know what they are."

But sometimes even supplychain professionals can struggle to pinpoint where risks might exist. Charlie Clark, chief executive of Rosslyn Analytics, recently told a number of chief procurement officers (CPOs) that their companies were potentially exposed to trade sanctions imposed on Russia. "This was a risk many weren't aware of, because they did not believe they did business in Russia or with Russian companies," he said. "But analysis of data showed some suppliers, although based in other countries, were Russian owned. Armed with this information, the CPOs were able to communicate this risk to their boards and take action to mitigate it."

Organisations have started to recognise that CPOs can offer strategic as well as operational advice, which has created more career opportunities for people in this area, said Joanne Till, managing director of Cordant Recruitment. "It [this recognition] has seen more requirement for people to take up boardlevel positions."

There has also been a slight increase in interest in nonexecutives with supplychain experience, she added.

Sue O'Brien, chief executive of Norman Broadbent, the search firm, agreed but pointed out that few have put themselves forward. "They have not been encouraged. I would also say that these people are not well known to the executive search community. It is up to them to step forward and articulate what they have to offer."

Supplier helped to cut costly callouts

About 40% of Lavendon's annual spending is swallowed up by goods and services so it makes sense for the equipment rental company to pay close attention to its relationship with suppliers, said Don Kenny, the chief executive.

"I like to think of them as an extension of our employees," he said. "The best suppliers are people you can rely on to do a good job, give you good value for money and, perhaps most importantly, bring innovation and proactivity to the business."

For instance, when Lavendon realised it was spending a lot of money on hydraulic hose repairs, it worked with its supplier to reduce the number of expensive callouts by buying equipment to do much of the maintenance itself. "This was a joint initiative between us and our supplier," Kenny said.

"It still gets the odd callout from us in emergencies, but otherwise it now largely supplies us with raw materials and equipment. It is a great example of innovation and creativity on the part of the supplier."