Source: *The Business Times,* p24
Date: 30 April 2015

Corporate governance in Muddied Waters

From short-sellers to whistle-blowers, to 'stealth' cyber attacks, companies today are subject to intense scrutiny and would do well to be prepared. BY LAWRENCE LOH

WE are on the cusp of a potentially novel trend in corporate governance. For too long, it is always the shareholders demanding more disclosure, more transparency, better governance from the company's management. The board is used as the potent instrument which can enforce stronger accountability and responsibility from such management.

Enter Muddy Waters Research. This short-seller cum whistle-blower now rains down on companies to expose allegedly dubious business practices and lapses in corporate governance. It even has the audacity to proclaim its short position in the targeted company and its intent to bring down the stock price so as to make for itself a tidy profit. Its initial array of targets includes listed Chinese companies and recent attacks cover familiar global entities like Olam International and Noble Group.

Whistling duo

Muddy Waters' success rate has been mixed, but in most cases the initial downwards share reactions were more than enough for it to cash in huge gains. In the process, the targets were also often queried by the respective stock market regulators, particularly to account for the unusual price movements.

As if the waters are not muddy enough, another whistle-blower Iceberg Research joined the fray and attacked Noble Group. In this case, it stated that it is not a short-seller.

But the game-changing feature is that Iceberg Research is anonymous; it is hidden in the cyber world where it operates and disseminates far-reaching information. And most notably, shareholders appear to take heed of Iceberg's reports. And strangely, information from nowhere seems to be getting somewhere.

Revolt

Naturally companies being hit would fight back. With these whistle-blowers, the companies concerned suddenly find that they have to answer to the charges. Many have, in fact, spent laborious hours and valuable resources to refute the points of contention.

Interestingly, in the recent incident of Noble Group, shareholders at the annual general meeting voted overwhelmingly to adopt the financial statements despite the claims proffered by Muddy Waters and Iceberg. However, there were debates on how the company might have pushed itself through the questioning at the meeting.

The series of offensives by the whistle-blowing duo may mark a turning point in the global corporate governance landscape. The traditional chain of accountability by companies to shareholders and regulators stands moderated by third-party analysts that often have vested interests. These are different from the usual range of brokerage-related or portfolio-based analysts who issue buy, sell or hold recommendations.

The Muddy Waters and Iceberg type of players may well be a new addition in the corporate governance ecosystem.

Who cares?

A first question that often comes to mind is: My company is not a high-profile entity in a sensitive and volatile industry (we don't trade commodities, we don't run supply chains) – should I care?

It is not always and only the big companies that get attacked. Any company can be vulnerable. As long as your company is listed and traded, it is easy for anyone to pick up the red flags in this digital era.

The key point to note is that the invaders need not be high-profile players like Muddy Waters or Iceberg. We are likely to see advocates and activists, often operating as individuals, who are now emboldened and likely to go beyond the isolated queries to be even more comprehensive, holistic and systematic in taking on companies. And for these, it may even be the smaller companies that are implicated.

Companies such as Noble have fought back with point-by-point rebuttals and legal action. PHOTO: REUTERS

Indeed we may well have lurking in the pipeline many mini-Muddy Waters and mini-Icebergs. Anyone, any outfit can be such players.

So what?

Another question is probably: What should I do when my company is attacked?

Of course, if all the claims are baseless, you can simply ignore them. But the problem is that investors may sometimes be persuaded by these claims, especially if they come along with "facts and figures".

One key choice you have to make is whether to remain on the defensive or even to mount an offensive.

From a defensive viewpoint, companies may simply try to explain their way out. In Noble Group's case, point-to-point rebuttals were given to the charges by Iceberg. Shareholders are normally reasonable people but if their pockets are hit, they may join the upheaval. Thus it is necessary that the company takes the due diligence to be as forthcoming as possible.

Often, it may serve the targeted companies better to take the offensive. Legal actions may be taken against the whistle-blower for false claims. Even in the case of anonymous Iceberg, Noble Group purportedly knows who the perpetrator is and has been taking the legal route.

If your company has some major shareholders who can stand firm on your side, it would be even better. In the Olam case, Temasek Holdings increased its stake in the company and this boosted the confidence in the company. But this is probably an exception and not the norm for many other companies.

Of course the critical step is to engage the media, especially if the attack has received significant attention. Noble Group's CEO has actively employed the media to tell the company's side of the story.

Who's next?

You may then ask: How to make my company less vulnerable? Indeed, how do I tell if we are next in line for an attack?

The answer is probably: What is in your "BAG"? This refers to your practices in Business, Accounting and Governance.

For business practices, the main issue is your revenue model. How is money made? Is there any complex web of cash flows that investors and analysts find hard to understand and may thus be basis for doubt? Has your company grown inordinately by acquisitions that seem improperly valued? Are there alliances that do not make sense to people outside the company?

For accounting practices, the general conventions should prevail. Are there controversial ways of accounting treatment that may be grounds for suspicion? Are there dealings that may be recorded and seem not to have occurred? Have assets been written off in extraordinary ways that are unconvincing? Are there assets carried that seem to come from expenses?

For governance practices, it is best for listed companies to observe the principles and guidelines in the relevant codes. For Singapore, there is the Code of Corporate Governance which is based on the comply-or-explain approach. It will indeed be quick and easy for assailants to determine where the non-compliances are and how these are explained (sometimes there may be instances where there are no explanations).

One major area of concern is usually board appointments which are often subject to intense scrutiny. Has the company, say, met the requirement for director independence if the chairman is not independent? Are there long-serving directors that may attract attention? Are executives excessively remunerated? Other areas may pertain to auditing which is often a hot button for shareholders. There may also be specific issues in disclosure such as related-party transactions which may be controversial.

Measuring up

Many countries do have assessment schemes that report the corporate governance performance of their listed companies. In Singapore, the Governance and Transparency Index (GTI) publishes the rankings and scores for corporate governance in all listed companies. The Singapore portion of the Asean Corporate Governance Scorecard reports the corporate governance results for the 100 largest companies by market capitalisation. Recently introduced, a new Governance Evaluation for Mid and Small Caps (GEMS) provides governance ratings for listed small and medium enterprises.

A starting point for potential attackers may be to look at those companies which have low scores or have dropped sharply in the relevant ratings. This may be an initial filter to detect major lapses. Naturally such a method is not foolproof as many global mega-lapses in corporate governance such as Enron, Satyam and Olympus did not seem to have red flags for several years prior to exposure.

Indeed companies should do self-assessment in corporate governance using the available instruments as developed by the respective rating organisations.

Stay ready

Amongst the three categories of practices – business, accounting and governance – perhaps governance is the mother of all the practices as it relates to leadership and sets the structures and processes to direct the conduct of the other two practices.

The best defence to potential attack is thus good corporate governance. It pays to plug the holes and make the company water tight.

Companies should form task forces to review the corporate governance situation. This is not just the job of the company secretary or investor relations function. The board should take the lead to steer the company to be less vulnerable.

It will be proper to work through scenarios and exercises to simulate potential attacks. What contingency plans does the company have in place? Is there a crisis response protocol? What are the communication plans?

As a well-known Chinese proverb goes: "It is easy to dodge the spear in the open, but hard to avoid a stab in the dark".

Yes, it is always good to be alert. The Scout Motto sums it well – "Be Prepared".

The writer is deputy head and associate professor of strategy and policy at the National University of Singapore Business School. At the School's Centre for Governance, Institutions and Organisations, he leads the Asean Corporate Governance Scorecard and the Governance and Transparency Index projects.