Cybersecurity: What Should a Board of Directors focus on?

June 02, 2015
Tania Djerrahian, Vanessa Coiteux

*In this, the second in our series of posts on the duties of Canadian directors and officers, **Vanessa Coiteux** and **Tania Djerrahian** discuss some of the key issues that directors need to focus on in the rapidly developing area of cybersecurity. The article considers some of the cybersecurity concerns expressed by securities regulators and proxy firms as well as some of the considerations that should go into an effective cybersecurity strategy.*

Most companies today depend on networks, computers and the Internet to help manage their business. While digital technology has many benefits, it also has the disadvantage of exposing companies to cybersecurity breaches. Historically, many viewed the risks associated with cybersecurity as risks to be entirely managed by a company's information technology (IT) department. However, given the number of companies in various industries that have experienced cyber-attacks in recent years, and the serious consequences of many of those attacks, boards of directors may, depending on the facts and circumstances surrounding their company, consider elevating such risks to enterprise-wide risks (as was the case for financial risks following the Enron scandal). As will be discussed below, there are a number of reasons why boards of directors of public companies may want to oversee the management of cyber risks and a number of practical ways of doing so.

Some Reasons Why Boards May Want to Oversee the Management of Cybersecurity

Impact on the Company's Bottom Line

The incidents involving Target, Sony, and JP Morgan are good examples of how a cybersecurity breach can significantly impact a company's bottom line. Investigation and remediation costs related to a cybersecurity breach (even an unsuccessful one) can be extensive, not to mention costs related to lawsuits from customers, suppliers and shareholders and costs related to the disruption to the day-to-day business. However, those costs are not the ones that keep a board of directors or the management of public companies up at night: the most serious threat to the bottom line is reputational damage and the loss of customer loyalty. It can take months, if not years, to recover from such a loss of confidence.

Securities Regulators Encourage Companies to Consider Disclosure of Cybersecurity Risks

Securities regulators in both Canada and the U.S. are concerned with cybersecurity and encourage companies to (i) assess cybersecurity risks and put controls in place to deal with those risks; and (ii) consider whether they need to disclose those risks and controls as well as any material cyber-attacks as part of their public disclosure. In Canada, the Canadian Securities Administrators' (CSA) **Staff Notice 11-326**, **adopted in 2013**, provides the CSA's views and suggested actions regarding cybersecurity. In the United States, **CF Disclosure Guidance: Topic No. 2** issued by the Securities and Exchange Commission (SEC) provides a detailed outline regarding the Division of Corporate Finance's views on

disclosure obligations relating to cybersecurity risks and cyber-incidents. The disclosure guidance in the U.S. may raise concerns for U.S. public companies as the detailed guidelines may be read to require detailed cybersecurity disclosure which could provide useful information to potential hackers and competitors. To respond to this concern, the SEC's staff acknowledges that "detailed disclosures could compromise cybersecurity efforts" and that "disclosures of that nature are not required under the U.S. federal securities laws". However, despite the acknowledgement, from a practical perspective, there remains a challenge as to where to draw the line and still be in compliance with the guidelines. In Canada, though the CSA's Staff Notice 11-326 is not as elaborate as the SEC's guidance, companies also have the difficult task of balancing disclosure that is sufficient for the purposes of legal compliance against disclosure that may provide a road map for a cyber-attack.

Negative Recommendations from Proxy Firms and Impact on Ability to Get Re-elected

In 2014, following a cyber-attack on Target, Institutional Shareholder Services recommended that the shareholders of Target withhold their vote in favour of the members of the board of directors who were on the company's audit and corporate-responsibility committees on the basis that they failed to properly manage the cyber risks faced by the company. Though Glass, Lewis & Co. did not make the same recommendation regarding Target's directors, it is clear that boards who fail (or are seen to have failed) to manage cybersecurity issues adequately may be at risk for a negative recommendation from proxy advisory firms. A negative recommendation combined with the application of a majority voting policy (now required for all TSX-listed issuers), could have the potential to put at risk some directors' re-election, not to mention potentially exposing the directors to liability.

Potential Responsibility for Breach of Duties

In the U.S., a number of derivative suits have recently followed in the wake of cyber-attacks. This development is evidence of shareholders' increasing willingness to sue directors for a breach of their duties in relation to the management of cyber risks. For example, in *Palkon v. Holmes* (D.N.J. 2014), often referred as the Wyndham case, a shareholder of a Delaware incorporated company tried to bring such a suit following three separate cyber-attacks on the company during a two-year period that allowed hackers to obtain the personal information of over 600,000 customers. The shareholder alleged that the directors had breached their duties to the company and wasted its assets. In Canada, a breach by directors of their fiduciary duties or their duties of care could also lead to a suit against directors based on a derivative action or an oppression action, both of which allow a court to make any order it considers appropriate, which may include an order that the directors pay compensation.

Whether in the U.S. or Canada, poor oversight of the management of cybersecurity could make it difficult or impossible for a board to rely on the business judgment rule in the event of a lawsuit. The business judgment rule provides that a court will defer to the business judgment of the directors if they took the time to inform themselves of issues and impact on the company, and acted with honesty in the best interests of the company. In *Palkon v. Holmes* – the "Wyndham" case referred to above – the board's management of the cyber crises and the application of the business judgment rule led to the dismissal of the derivative suit at the motion stage. As a matter of illustration, in that case, the board of directors held 14 quarterly meetings in which it discussed the cyber-attacks and company security policies and proposed security enhancements. The board of directors also appointed the audit committee to investigate the breaches, and that committee met at least 16 times to review cybersecurity. The company also hired a technology firm to recommend security enhancements, which the company had begun to implement. In contrast, in a case where liability is triggered by an omission, it could be significantly more difficult to invoke the business judgment rule in the board's defence. For example, if there is no risk management system in place for dealing with cyber-attacks, it could be argued that this inaction or omission should not be protected by the business judgment rule since there was no "decision" of the board's members.

Practical Ways to Oversee Cybersecurity

There is no “one size fits all” solution in term of overseeing the management of cybersecurity, but rather a set of steps that boards may want to consider so that they can arrive at the solution that works best for their company. These steps consist of:

- evaluating the risk;
    - considering the cybersecurity measures that should be put in place;
    - considering the cyber-attack response plan that should be adopted; and
    - considering what is the required level of disclosure in the circumstances.Whether each of these steps, or even each of its components, will be taken will depend on the board and its appreciation of the facts and circumstances surrounding the company.

Evaluate the Risk

The first phase in evaluating the risk is determining who will play a key role in the oversight process: the board itself, the audit committee, the risk committee or another committee (i.e. IT committee). As part of this step, the board may want to determine whether the members of the board or the committee have the requisite knowledge or expertise to understand IT issues and how they translate into business issues. If IT knowledge or expertise at the board or committee level is not up to par, the board or the committee may need to consider hiring independent IT specialists to help it make reasonable and informed decisions as well as inquiries with senior management.

The second phase in the evaluation process is understanding what are the most sensitive data assets of the company (from a competition, privacy or disclosure perspective) and what may put them at risk. Here, the board or the committee may require information on:

- where the risk is coming from (e.g. does the risk come from the company’s own IT system only, the use of a cloud, or from the IT system of those that do business with the company such as third-party suppliers and partners?);
- how well the detection systems work;
- any past cyber breach attempts and responses taken;
- what assets, information or data are at risk;
- the estimated cost and expenses the company will incur if any of the “at risk” items are affected by a successful cyber-attack; and
- the coverage the company has under its insurance policies with respect to cyber breaches (many D&O policies and general commercial policies do not cover electronic data breaches).

In order for the board or committee to fulfil its duties, it is essential that it be provided with sufficient, appropriate and timely information on relevant IT matters and assets. However, board or committee members may not want to wait for such information to be provided to them: depending on the facts and circumstances, they may need to be proactive and ask questions.

At every stage, cyber risk assessment should be done within a proper “risk framework”. In January 2015, the Committee of Sponsoring Organizations of the Treadway Commission released guidance on how its 2013 framework and **2014 Enterprise Risk Management—Integrated Framework** can help companies evaluate and respond to cybersecurity risks.

Consider the Measures that Should be Put in Place

The next step is for the board or the committee to consider whether additional protection measures should be put in place. As recommended in **National Policy 58-201 – Corporate Governance Guidelines**, a board’s mandate should not only identify the risks but also ensure that appropriate systems are put in place to manage these risks. Thus the board or the committee will want to inform itself with respect to questions such as the following, as appropriate:

- whether the security systems and IT measures put in place to protect the assets, information or data is proportionate to the exposure faced by the company should such assets, information or data be compromised by a cybersecurity breach and/or exposed;
- whether additional measures ought to be put in place including employee education on cybersecurity, supplemental insurance policies, the imposition of contractual security requirements on third parties who have access to or are connected to the company's electronic data and new security systems;
- whether there is sufficient and appropriate reporting information provided to the board;
- who will be tasked with implementing the additional measures and reporting back to the board or the committee and whether that person is given sufficient power, budget and support to do so; and
- how often and under what circumstances the board or committee should be briefed on cybersecurity and how such review analysis and review process is documented.

Consider the Response Plan that Should be Adopted

Given that it is likely a situation of when a cybersecurity breach will occur rather than if it will occur, the board or the committee may also want to consider adopting a response plan in reaction to a cybersecurity breach. As with any crisis, a poor response can be as damaging as the events that led to the crisis. Here, the board or committee may want to determine:

- what the elements of the plan should consist of, including communication plans, legal disclosure obligations, plans to minimize business disruptions and damages;
- if outside advisers such as legal counsel and public relations specialists could help with the creation and execution of the plan and with privilege issues;
- within the company, who should be responsible for implementing the plan and reporting back to the board or the committee and whether that person is given sufficient power and support to do so; and
- how often the plan will be tested and adjusted.

Consider the Appropriate Level of Disclosure Following a Cyber-Incident

As with any incident affecting a public company, public disclosure following a cyber-incident is key for a company to preserve its brand and reputation, limit the board of directors' potential liability and manage the other potentially large costs associated with the incident. Here, the board or the committee may want to ensure that management is in a position, if needed, with the help of outside legal counsel, to

- efficiently determine the level of materiality of the attack and whether the incident constitutes a "change to the business, operations or affairs" of the company in order to determine whether a press release should be issued immediately; and
- determine the level of work that needs to be completed in advance of a public disclosure (i.e. identify the scope of the cyber-attack – including its impact on merchant and customer data – where the intrusion came from, whether it was due to a failure of the company's protection measures, what remediation work should be put in place, the available means for customers or other affected stakeholders to get additional information and whether the risk factors and other related public disclosure are sufficiently broad to include all the potential consequences of a data breach).

In addition, when a company is due to file its continuous disclosure documents such as its financial statements, Management Discussion & Analysis or Annual Information Form, the board or the committee should question whether an update regarding such cyber-incidents or a material fact regarding cybersecurity of the company should be disclosed. Even though most public companies would prefer to limit disclosure as much as possible, board members should bear in mind that the best approach is sometimes to include a complete disclosure (including potential consequences) when the spotlight is not

on the company rather than having to build a disclosure framework, including material details of an attack, when everyone is looking and some stakeholders are trying to use the opportunity to carry out their own agenda. In addition, as was the case in many of the recent incidents, the cyber-attack may first be detected by a government agency or a banking partner rather than the company that is under attack, thereby putting even more pressure on the board and management to make sure (i) the company's initial disclosure is complete and up-to-date and (ii) there are plans in place which provide for the efficient disclosure of any new material change or material fact, as applicable, in compliance with securities laws in a way which will limit damage to the company's reputation

Depending on the facts and circumstances surrounding a company, the stakes associated with cyber-attacks can be high. Members of a board of directors may not want to wait for an attack before considering cybersecurity risks facing their company. During a cyber-attack, when everything is moving quickly and in real time, preparedness is key as directors usually won't have the luxury of time when trying to understand, analyze and react to the breach.