2018: A Year of Living Dangerously

How New Regulations and Technology Disruption Will Challenge the Board and C-Suite

How New Regulations and Technology Disruption Will Challenge the Board and C-Suite

To officers and directors of Canadian companies that are SEC registrants – take note of new requirements for managing cyber breach risk. For all Canadian organizations – take note that the new Canadian privacy legislation is a bear.

This article summarizes a handful of new regulations aimed specifically at the manner and robustness of how exchange-listed companies address and respond to a cyber event - the "demon-child" of the digital revolution that has swept our globe. Our objective is to raise the awareness that, regardless of an organization's actual experience with a cyber incident, the laws have changed and the financial and reputational penalties of poor management and oversight can and will be swift and painful.

In addition, we will provide with a handful of specific and practical actions to take to respond to the challenges presented by the digital revolution from the perspective of the C-suite and the boardroom. This is not meant to be an exhaustive conversation but rather a handful of observations and recommendations that are straightforward and actionable immediately. These of course will change as each entity begins what the proverb describes as *"the journey of a thousand miles".*

Why are these regulations a big deal?

The year 2018 might go down in the history books as the year that regulators put a stake in the shifting sand that characterizes the digital landscape for virtually all commercial enterprise around the world. In the US, the *Securities Exchange Commission ("SEC")* - arguably one of the more feared and respected national regulators - released its updated guidance on cyber security matters calling for higher standards for all registered entities i.e. public companies that list on US stock exchanges. Effective February 21, 2018, all listed companies are expected to demonstrate a comprehensive array of capabilities that will ensure the organization effectively addresses how officers manage cyber risk and how board directors oversee these efforts.

The new standards also call for much higher levels of care with respect to how companies track and monitor their insider trading and selective disclosure processes and protocols in addition to raising the bar on how all of these actions are described in the company's MD&A section of their required filings.

It is unclear as to how successful all companies listed on US exchanges (including the 162 Canadian companies that are listed in the US) will be in complying with these new standards. That said, unlike our collective experiences complying with the tenets of Sarbanes-Oxley and its Canadian equivalent Bill 198 or C-Sox, many Canadian (and US) companies will likely significantly struggle with meeting these new requirements. One of the major factors contributing to this observation is the lack of available expertise in the boardroom and to a lesser extent, the C-suite.

North of the border, recent moves by Canadian regulatory authorities are less about how a company manages its cyber security risk per se and more about how Canadian organizations meet new legislation designed specifically to protect individual privacy rights.

On November 1, 2018, the federal government's revisions to the national **Personal Information and Protection of Electronic Documents Act** or "PIPEDA" comes into force. The objectives of these much-anticipated revisions include; harmonizing the disparate range of provincial regulations relating to the protection of individual privacy rights; raising the profile of the federal Office of the Privacy Commissioner

("OPC") and making all of Canada largely compliant with the key principles of the *General Data Protection Regulation* (or "GDPR") that went into force in the Eurozone on May 25, 2018.

The revised PIPEDA details a number of stringent requirements relating to content and manner that is used to notify any and all individuals whose personal privacy *has been or has potentially been*, inappropriately shared, accessed or lost due to any actions, not just those that are a result of a cyber event i.e. a lost company laptop or a memory stick containing customer data. These requirements are explicit and will create significant challenges for organizations to execute due in part to the comprehensiveness of the standards and the legal and reputational implications of these notifications.

In addition to reporting a real or potential privacy breach to affected and potentially affected individuals, organizations will be required to submit regular reports to the OPC detailing the organization's entire operation of the privacy breach framework. The form and content of this reporting to the OPC is explicit and will be used to confirm compliance with the regulations.

The new law also requires that all organizations establish and maintain a breach notification log that contains details of the circumstances of the privacy breach (real or potential), the date the breach was discovered, the date when the breach occurred and the steps taken to remediate the privacy breach (as an example).

Notwithstanding the implications of a revised PIPEDA, it is worth noting that those organizations who operate in the Eurozone and who capture, record and use the personal data of any resident must also comply with the sweeping and broad regulatory GDPR regulations that came into force this past May. Penalties for failure to meet these requirements, which include a maximum 72-hour breach notification threshold, are draconian in their size (ex. 20 million Euros or 4% of global sales whichever is larger.

While Canada's PIPEDA does not have such outsized penalties for non-compliance, admitting failure to comply with PIPEDA and accepting the fine of $100K per violation would just be the starting point for plaintiff's statement of claim in class action litigation which is expected to blossom in this new regulatory environment.

We can respond easily to these regulations, can't we?

Following the tech bubble crisis, the introduction of Sarbanes-Oxley and the Canadian equivalent Bill 198, introduced the term "financial literacy" a.k.a. knowing how to read and understand financial statements. It is easy and fair to say that this new requirement (and the attestation by the CEO and CFO) was a relatively easy regulation to comply with given both the specificity of the regulation and the ample supply of experts (i.e. accountants) who could be recruited to join senior management teams as well as boards of directors.

The same cannot be said of these new privacy and cyber related regulations because they do not have the same level specificity and the supply of appropriate experts to serve on boards is scarce, and will require boards to tap into a non-traditional talent pool. To illustrate this point, take the results of a 2017 survey of US companies in which 72% of board directors said they needed more cyber expertise on their board. Of this total, 33% admitted they had none and the remaining 39% said they had some experience but needed more.[1] So, if roughly three quarters of America's boardrooms are under-equipped to provide oversight of compliance with these new regulations, then it doesn't take a crystal ball to predict a range of potential

[1] *2017 Annual Corporate Directors Survey*, October 2017 by PWC

outcomes – most of them involving loss of business, damage to reputations and of course, messy and costly litigation.

What actions do we take now?"

One of the first actions all entities need to take is to evaluate the robustness of their risk management capabilities and quickly identify their strengths and more importantly, their vulnerabilities. Your specific organization might not be able to comply with all of these new regulations in the immediate term but you will need to comply with those that create an existential threat to your organization. More specifically;

- For the C-Suite, begin by implementing a disciplined, methodical and common-sense approach designed to identify the 2 to 3 biggest vulnerabilities to the top 1 to 3 ranked digital assets of your organization. You will need this in order to identify the top 2-3 must-fix-now initiatives. Be prepared to explain to your board, regulators and other key stakeholders the logic behind your approach and keep a keen focus on completing these specific initiatives.

- For Board of Directors, carefully listen and evaluate the approach that management has used to address new regulatory edicts and maintain the intensity of your oversight of these initiatives. Regulators favour honesty, humility and transparency and likely recognize that no organization can be "totally compliant" at any one time. That said, they have little patience (and a lot of disdain) for obfuscation designed to paint a picture of something that is not reality.

While the limitations of this article prevent inclusion of a fulsome list of actions to take now, the following offers a couple of thoughts that will help frame how you create an action plan:

1. Accept the fact that if your board or c-suite is composed of people who remember disco, the floppy disk or who have never personally been accountable for designing, leading or fixing a major technology implementation project and who do not have any formal experience in pre-post risk analysis then accept that your skills assessment will identify a significant gap.

2. Create a shopping list of skills and experiences that would characterize someone who would fill the competency gap on your board. Candidates do not have to be bonified "experts" but they at least need to be knowledgeable and conversant in topics such as data analytics, artificial intelligence, IoT and perhaps robotics. I would ask management to provide you with the list of topics that they think might be relevant but use someone independent to validate the list, until you have the requisite expertise on your board.

3. Absolutely accept the fact that, to fill this competency gap, you cannot use your traditional sources be they personal contacts or traditional search organizations to find potential candidates; because this is simply fishing in the same ponds that they have for years. Moreover, it is extremely unlikely they will take the chance of presenting someone who does not meet all of your requirements because their business model does not include do-overs. When was the last time a retained search firm proactively showed you a profile of someone who they think might add value and was very different from your existing composition and do it for free?

4. Get busy now. There is a finite supply of talent globally that has the requisite skills, experience, maturity and capacity to be an effective board member responsible for being a "technology / innovation / cyber" expert. It is best to be among the early leaders in order to get to the already scarce talent first!

In this case, patience is not a virtue… it is a sin.

We began this conversation talking about how these new regulations are going to be much more difficult to comply with than those that resulted from the accounting crisis of the last decade. The analysis provides a shot across the bow for those organizations that choose to take no action and hope for other another company to get caught first. To be clear, hope is not an effective strategy. It is however one of the reasons that some entity will appear on the front page of the newspaper (rarely a good thing) or on page 1 of a Statement of Claim for Damages (never a good thing).

We also talked briefly about the unprecedented nature of the challenges that are unique to the risks that the digital revolution is bringing to the doorstep of virtually every business in the world. To provide a broader context beyond complying with new regulations relating to cyber, privacy and disclosure risk consider the following. In a 2018 report produced by Innosight[2], the authors highlighted the fact that the lifespan of component companies on the S&P 500 index are on a rapid descent moving from 33 years in 1964 to 24 years in 2016 to 12 years in 2027. Their blunt conclusion, 50% of S&P 500 companies will be replaced over the next decade. For those currently in the C-suite and the boardroom – that sound you hear at your door is creative destruction and it is relentless. Every entity needs to get help in their C-suite and their board in order to ensure they come out on the right side of the 50/50 bet over the next decade.

About the Author

Lloyd Komori has worked exclusively in the risk management space for over 3 decades as a derivatives trader, Chief Risk Officer and instructor of a board director education program and as an active board director. He is also a student as well as an expert in cyber risk and artificial intelligence and spends a great deal of his time expanding his toolkit and insight in order to help his boards deal with the implications that disruptive technology has on risk, strategy and governance.

[2] a consulting firm founded by HBS professor Clayton Christenson and Mark Johnson