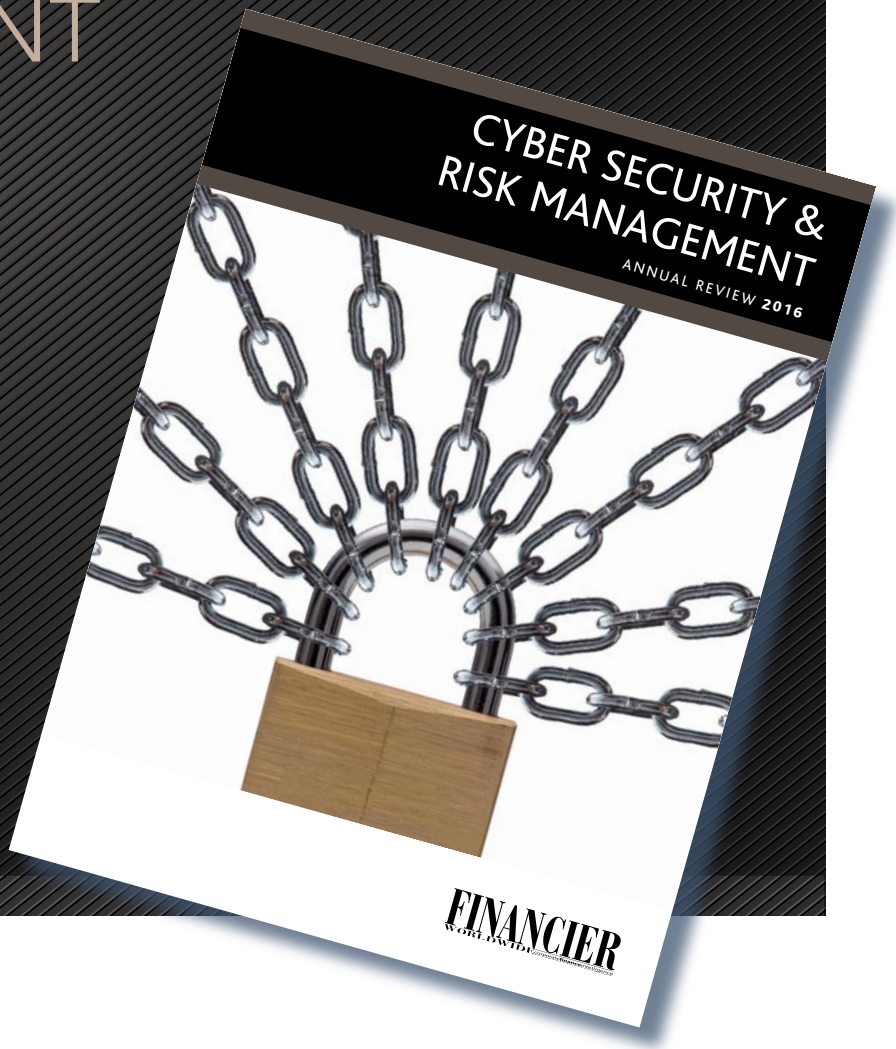
ANNUAL REVIEW

CYBER SECURITY & RISK MANAGEMENT



REPRINTED FROM
ONLINE CONTENT
JULY 2016

PREPARED ON BEHALF OF

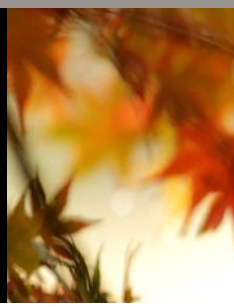
STIKEMAN ELLIOTT

STIKEMAN ELLIOTT LLP

FINANCIER WORLDWIDE corporatefinanceintelligence

CANADA

VANESSA COITEUX
STIKEMAN ELLIOTT LLP



Q HOW WOULD YOU SUMMARISE TODAY'S CYBER-RISK ENVIRONMENT? WHAT NEW RISKS HAVE EMERGED IN THE PAST 12-18 MONTHS?

COITEUX: I would say that in the past 18 months, we have witnessed a number of important developments. These include a jump in extortion-driven attacks where hackers use sensible information to blackmail organisations, new risks emerging from poorly planned or executed cloud service integrations or the use of non-secured cloud based solutions, an increase in risks posed by third-party suppliers and contractors having access to a company's infrastructure, the proliferation of new and mass repackaging of ransomware, and security incidents related to enterprise connected personal and mobile devices (BYOD).

Q WHAT IMPACT HAS THE CLOUD HAD ON DATA SECURITY? WHAT SHOULD COMPANIES BE CONSIDERING WHEN TRANSFERRING DATA STORAGE TO THE CLOUD?

COITEUX: The cloud computing landscape has grown intensively in the last few years because of its relatively low cost and its functional and economic advantages over traditional storage methods. However, one thing to remember is that a company outsourcing data storage to a cloud service provider does not outsource its privacy obligations under Canadian privacy laws. As such, one primary concern is to ensure that the information sent to the service provider is protected. What are the safeguards used by the service provider to protect the data? What monitoring does the company do to make sure those safeguards are being implemented and followed? There are a few ways to reduce a company's risk profile when using the cloud. Companies should be selective in the type of data transferred to the cloud. They should ask questions about the jurisdiction in which data is being stored and the legal and regulatory privacy requirements governing this jurisdiction. They should ensure that sufficient safeguards are implemented by the cloud provider, such as through contractual representations and covenants and rights of audit and access, as the case may be. Finally, they should include a clear allocation of responsibility and liability among the service provider and the client in the contractual documentation to avoid any gap or disconnect.

CANADA • VANESSA COITEUX • STIKEMAN ELLIOTT LLP

Q COULD YOU OUTLINE THE PRINCIPLES OF DATA PRIVACY LAWS IN CANADA, AND THE DEMANDS THEY PLACE ON COMPANIES TO IMPLEMENT SECURITY MEASURES AND FOLLOW NOTIFICATION REQUIREMENTS? HOW CHALLENGING IS IT FOR COMPANIES TO MAINTAIN REGULATORY COMPLIANCE?

COITEUX: In Canada, the collection, use and disclosure of personal information in the private sector is either governed by federal, provincial or sectorial legislation, depending on many factors. All privacy laws, whether federal and/or provincial, require companies to implement sufficient security safeguards designed to adequately protect personal information. That said, most data privacy laws in Canada only establish general guiding principles to be followed by Canadian organisations. Currently, Alberta is the only Canadian province imposing a notification obligation in case of breach. However, the new *Digital Privacy Act* (DPA), once the regulation implementing its application is adopted, probably in Autumn 2017, companies that are subject to federal law will be required to, among other things, notify the Privacy Commissioner of Canada and affected individuals of any breach of their security safeguards involving personal information, if such a breach meets certain thresholds. They will also need to establish and maintain a record of every breach of their security safeguards involving personal information. While some companies were already notifying affected individuals on a voluntary basis, companies governed by the DPA will now be forced to do so. These new breach notification provisions will definitely result in new costs, risks and challenges for Canadian companies, including an increased pressure for transparency.

Q WHAT STEPS SHOULD COMPANIES TAKE TO ESTABLISH APPROPRIATE PROCESSES AND POLICIES TO MANAGE CYBER RELATED RISKS? HOW IMPORTANT IS IT TO ADDRESS THE ORGANISATION'S RISK

COITEUX: It is extremely important for a company to have a carefully crafted cyber security plan, including both a data security policy and an incident response plan. The data security policy should focus on three aspects. First, governance – ensuring that senior management and board members are accountable and allocate responsibility and resources. Second, industry standards – ensuring that the infrastructure is up to date with current security standards. Third, and, most importantly, corporate culture – raising level of awareness among the employees. Most security professionals would agree that many companies' weakest link is, more often than not, their people. As

"Board members now realise that they have to take active steps if they want to fulfil their fiduciary duties."

CULTURE, SO THAT EMPLOYEES UNDERSTAND THE ROLE THEY PLAY IN KEEPING SYSTEMS SAFE?

such, organisations must train their employees so they can understand the importance of cyber risk management, identify potential sources of cyber security breaches and know how to react when one happens.

Q INSURANCE IS A KEY PART OF MANAGING CYBER RISK. HOW ARE INSURANCE PROVIDERS ADJUSTING OR ENHANCING THEIR INSURANCE SOLUTIONS TO MEET MARKET DEMANDS? WHAT TYPES OF POLICIES ARE AVAILABLE TO HELP MANAGE THE DOWNSIDE?

COITEUX: Market demands are ever changing since new risks emerge every day and insurance companies build corresponding policies designed to address such risks. If everyone agrees that the average cost of a cyber breach increases year after year, it is still a challenge for insurance providers to adequately quantify the damages and related costs associated with a cyber attack and, incidentally, accurately assess their risk. Given the lack of historical data, especially in Canada, it is difficult to put a monetary value on cyber risk. Another challenge for insurance providers is the dynamic nature of cyber risks, which forces them to adapt their insurance offering to ensure coverage is always up-to-date. While it is true that cyber liability insurance is modular, the basic offering generally includes two components: first-party coverage for the companies' own losses and third-party coverage for an insured's third-party losses. Other cyber insurance features, such as business continuity coverage, may be added to cover specific business risks and needs. As a result, a cyber liability insurance product is not a one-size-fits-all product that suits every company's needs, but rather is tailored to each company.

Q WHAT CONSIDERATIONS SHOULD COMPANIES MAKE WHEN EVALUATING CYBER INSURANCE COVERAGE, INCLUDING PRICING, POLICY PROVISIONS AND EXCLUSIONS?

COITEUX: It is no secret that, when evaluating any insurance product, a company has to look at inclusions and exclusions carefully. Since cyber crime is a risk that is so different to what insurers typically cover, traditional provisions of general liability insurance policies will sometimes burden the insured with unexpected exclusions. For example, is cyber crime considered terrorism? What if it is state sponsored? Other considerations that are specific to cyber risks also need to be taken into account. For example, would a company be insured against the damages resulting from malware installed on the company's systems before the insurance was taken but which resulted in a cyber attack after the company was insured? Is the policy retroactive? Furthermore, as cyber insurance is quite complex, with tens of different risks

coverages offered to companies, coverage needs to be assessed on a case-by-case basis based on every company's infrastructure, appetite for risk and risk profile.

Q GOING FORWARD, MAJOR CYBER THREATS ARE ONLY LIKELY TO INCREASE. DO YOU BELIEVE CYBER RISK MANAGEMENT WILL CONTINUE TO CLIMB THE BOARDROOM AGENDA?

COITEUX: Based on experience, in most organisations, boards only have one technology related discussion per year, or even less. However, we believe this is set to change, since we have recently noticed a rise in cyber security related questions asked by board members. The increase in the number of cyber attacks year after year, and the fact that technology and types of attacks evolve so quickly calls for more regular discussions on this topic. Board members now realise that they have to take active steps if they want to fulfil their fiduciary duties. In the current business landscape, breaches are inevitable but boards can mitigate risk and damage by staying informed and ensuring that, in the event of a breach, their companies are as prepared as possible to respond.

STIKEMAN ELLIOTT

STIKEMAN ELLIOTT LLP

www.stikeman.com

Vanessa Coiteux

Partner
Stikeman Elliott
+1 (514) 397 3681
vcoiteux@stikeman.com

Vanessa Coiteux is a partner in the Montréal office of Stikeman Elliott LLP. Her legal practice focuses on securities, public and private mergers and acquisitions and corporate financing. She specialises in cyber security and advises public and private companies on legal, ethical and governance issues. Ms Coiteux advises clients on a wide range of privacy, data security and information management matters, including information security breach responses, compliance and disclosure, and provides opinions on best cyber security business practices. She holds a L.L.B. & B.C.L. from McGill University.

www.financierworldwide.com