CHARTIS

White Paper

Cyber Risk In Canada, A Board Level Concern

Management of data and information security has moved beyond the information technology ("IT") sphere. Information security is now a corporate priority, with potentially far-reaching consequences for a company's operations, finances and reputation. Consequently, cyber risk has gained significant attention in boardrooms throughout Canada and the U.S. The *12th Annual Law and the Boardroom Study*, prepared by Corporate Board Member and FTI Consulting, Inc. explored the risks most concerning to companies this year. The study reported that data security topped the list for both directors and general counsel. Over the past four years, the level of concern over data security has nearly doubled. Reputational risk garnered the third highest percentage of responses in the same survey. Following the recent spate of highly publicized security breaches, and the resulting fallout from key stakeholders, it is no surprise that both cyber and reputational risk are key board level concerns.

With a company's reputation at stake, directors and officers need to ensure that their organizations are protected. There are a myriad of threats to intangible information and data, and an organization must instill appropriate policies and procedures to adequately protect those assets. The intense media scrutiny of these types of incidents only compounds the potentially negative impact of a security breach, even if the incident is handled properly.

Several factors have combined to make cyber risk a board level concern, including the frequency, severity and evolutionary nature of the threat; the complexity of the exposure; the increased focus on good corporate governance; the changing regulatory landscape; the specter of potential Directors and Officers Liability ("D&O") lawsuits emanating from these incidents (potentially putting board members at personal risk); and the glaring reputational exposure associated with data security and privacy incidents.

Emerging Trends

Despite ongoing advances in network and IT security, the frequency of data security breaches continues to rise. According to the *2011 TELUS Rotman Joint Study on Canadian IT Security Practices*, six times the number of breach incidents were reported by public companies in 2011 as in 2008. Recent studies in the U.S. show the cost of a data breach (per record) also rising steadily year to year, with the average cost of a breach involving personal data exceeding $7.5 million dollars for an organization in 2010.[1]

The onward march of technology amplifies the threat. Mobile technologies, for example, now provide points of entry for data breaches virtually anywhere. The loss of mobile devices with business information was the primary security concern identified in the TELUS Rotman study. Yet the vast majority of senior managers in Canada also said they recognize the opportunity mobile devices represent to their business. Businesses know they must assume the risks of mobile technologies -- and they know the risk will continue to balloon as new technologies enter the mix.

Cloud computing is another advance that is taking exposure to new heights. When companies move data to the cloud, they gain flexibly, cost savings and efficiencies -- but they relinquish control over data breach risks, entrusting valuable and sensitive data to a third party.

[1] Source: Ponemon Institute LLC, U.S. Cost of Data Breach, sponsored by Symantec Corp

A cloud provider's large aggregation of data can make it an especially tempting target for cyber criminals. Outsourcing to a cloud provider can also expose corporations to contingent business interruption losses if the cloud provider's data and services become unavailable. A recent example is the June outage of Amazon's Elastic Compute Cloud, which took down Netflix, Instagram, and Pinterest, among others.

Social media is adding new dimensions and complexity to the exposure. As people become increasingly comfortable with sharing information on public and private platforms, they don't realize the overall information that can be gleaned from seemingly innocuous postings when viewed in tandem. Additionally, hackers have attempted to capitalize on the trust that exists between users of social media sites to gain entry to infect computers with fraudulent links or phishing schemes. And, like mobile devices, social media too is here to stay.

Prohibiting its use via corporate policy is increasingly unrealistic. Social media can be a powerful marketing tool. Moreover, TELUS Rotman's research shows that organizations in Canada that attempt to block access to social networking for security reasons are experiencing more breaches than those that do not. It seems that proper policies and procedures, carefully communicated and monitored, will yield better results than attempts to block access altogether.

The modes of perpetrating data breaches are changing and advancing rapidly. There are scores of ways to breach data: Hackers target personal information for financial gain, while "hacktivists" attempt to make a statement with a network intrusion. An employee may absentmindedly leave a laptop with sensitive data on a commuter train, or post sensitive information online. A rogue administrator pursues company records for personal gain, or a vendor is inadvertently granted access to customer data. Social media allows information to seep beyond the company's scope of command. There is also a recent trend towards specifically targeted attacks. The threats are seemingly endless. And what might be coming down the road? McAfee Labs Threat Predications for 2012 forecast that, among other things, industrial threats will mature and segment; hacktivism and Anonymous will reboot and evolve; virtual currency systems will experience broader, more frequent attacks; and traditional spam will go legit, while spear phishing evolves into targeted messaging attacks. 2012 will also be the year for cyberwar, McAfee Labs predicts. With both the cause and motivation of incidents constantly changing, organizations must constantly monitor and adapt to the threat in order to effectively manage it.

Along with personal information, corporate intellectual property may be targeted.
In one of the highest profile attacks of this type to date, hackers believed to be working in China accessed Nortel's computer networks for close to a decade and downloaded piles of intellectual property -- including technical papers, research-and-development reports, and business plans. The hackers apparently stole passwords from top executives at the company and embedded spying software in such a way that the extent of the intrusion was not perceived for ten years.

As with the example above, it is not unusual for attacks to go on for months, even years, undetected. According to the *Verizon 2012 Data Breach Investigations Report*, 85 percent of breaches studied took weeks or more to discover.

What Constitutes Personal Information?

Adding to the intricacies of managing this exposure is the ever changing regulatory environment, and the widening net of what constitutes personal information and hence requires protection under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). The Act broadly defines personal information as any information about an identifiable individual, and is understood to include a person's name, address, birth date, social insurance number, ID numbers, income, ethnicity, blood type,

passwords, license plate number, interests, hobbies, habits, sexual orientation, medical records and history, and loan and credit information.[2]
A recent ruling by the Privacy Commissioner of Canada has made determining what falls under the definition of personal information more challenging. In *Gordon v. Minister of Health*, the Commissioner ruled that seemingly innocuous information may constitute personal information if it can be combined with other available information to make an individual identifiable. (In this case, the seemingly innocuous information in question was the home province of an individual who suffered an adverse drug reaction.)

"When analyzing personal information after a breach, one cannot focus narrowly on the specific information that was disclosed, but rather should take a contextual approach. When deciding whether personal information has been leaked, it is wise to ask whether, when combined with other information that may be available through public or private sources, the information could lead to individuals being identified and subject to a real risk of significant harm," advises Andrea Laing, a litigation partner at Osler, Hoskin & Harcourt LLP in Toronto.

Getting it right is critical, she adds, as any data that is deemed personal information becomes subject to privacy legislation and triggers applicable notification requirements (current or pending).

Class Action Litigation

Other compelling reasons for boards to take notice of cyber risks are the costs and reputational damage that can come with data breach and network intrusion incidents. These dual threats are manifest most glaringly in the class action lawsuits that have arisen from breaches in Canada.

In *Rowlands v. Durham Regional Health*, the Ontario Superior Court of Justice certified a privacy class action against the regional health department after a nurse it employed lost a USB thumb drive containing the personal and confidential health information on over 83,500 patients, specifically unencrypted private patient information relating to H1N1 flu vaccinations. The plaintiffs in the class seek $40 million in damages. The allegations include negligence and breach of the statutory duty to protect patient information. While the claim is grounded in the defendant's alleged breach of statutory duty pursuant to Canada's Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sch. A, the plaintiffs' also allege that the defendants had a duty to maintain the privacy of the class members and breached that privacy.

Another class action lawsuit arose from a large Canadian bank inadvertently sending internal faxes containing customer information to various external parties, including a wrecking yard. The statement of claim under the proposed action asserted that the bank breached its duty to customers to keep customer information confidential, that it was negligent in failing to do so, and that it breached privacy rights. A settlement agreement was ultimately reached after litigation commenced. Under the agreement, each class member was given a claim form to submit to the defendant setting out the details of any loss or damage it suffered as a result of the disclosure of personal information. In response, the bank would make a settlement offer to the claimant. It would also pay $100,000 to a registered charity and the costs of class counsel. The right of any individual plaintiff to file a claim for identity theft in the future was preserved. "Although the monetary damages were not so high when the case was ultimately settled, the situation was acutely embarrassing for the bank," Laing noted.

A third example demonstrating the growing commonality of class actions in Canada is *Jackson v. Canada.* In this case the Ontario Superior Court of Justice refused to strike a claim for breach of privacy in a proposed class action on the basis that the claim was novel. The decision was upheld by the Court of Appeals. The case involved some 366 staff members from an Ontario jail who sought certification against Correctional Services Canada for leaving a list of employee names and home contact

[2] www.torys.com

information in an unlocked cabinet in an unsecured hallway. When the list was retrieved months later, certain names were highlighted. Finding the law was “not finally settled in this area” the Superior Court refused to strike a pleading for the “novel” claim of breach of privacy. A settlement was ultimately reached under which individual class members received $1,000 to compensate for their breach of privacy. "This case is particularly interesting because of the sensitivity of the information in light of the context and the potential that someone was planning to do something malevolent with it," Laing said.

More recently, two memory sticks containing personal information were lost by Elections Canada, potentially putting personal information on up to 2.4 million Ontario voters in jeopardy. As of this writing, a province-wide class action has been launched against Elections Canada. The action seeks, among other things, financial compensation for individuals whose information was contained on the misplaced memory sticks.

Whether or not they are ultimately certified, class actions are costly to defend and can generate substantial negative publicity for an organization. Indeed, according to a recent study by the Ponemon Institute, the average time it takes to restore an organization's reputation after a breach is one year; the average loss in value of the brand among executives surveyed was $184 million to more than $330 million.

Notably, the class action cases noted here did not arise from the deeds of a malicious hacker a world away. Employees were the root of the problem. This underscores one of the great challenges of managing the data breach risk: the threat within an organization. According to the Open Security Foundation, nearly 40 percent of incidents tracked emanated from inside the organization.

Other Important Case Law Development

A 2012 case, *Jones v. Tsige*, has several implications for breach litigation and specifically cases arising from the actions of employees. In this case, a rogue bank employee repeatedly wrongfully accessed an individual's personal financial information while on the job. The individual whose information was breached suffered no monetary damages, but the Ontario Court of Appeal found that proof of harm to a recognized economic interest is not required to substantiate a claim under the tort of "intrusion upon seclusion." The court stated that nominal damages up to $20,000 may be appropriate in such cases[3]. While that is a relatively small amount, it can mount quickly in a class action situation. It remains to be seen whether *Jones v. Tsige* will unleash a wave of class actions for inclusion upon seclusion.[4]

Regulatory Landscape

Canada has two federal privacy laws. The Privacy Act, which imposes obligations on federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information and PIPEDA, which provides a framework for how private sector organizations may collect, use or disclose personal information about an individual in Canada in the course of commercial activities. While it initially applied only to personal information about customers or employees that was collected, used or disclosed in the course of commercial activities by the federally regulated private sector (e.g., banks, airlines, telecommunications companies), it now applies to most businesses in Canada.

British Columbia, Alberta and Quebec have enacted laws similar to PIPEDA to regulate the collection, use and disclosure of personal information by businesses and other organizations within their respective

[3] Jones v. Tsige, 2012 ONCA 32 (CanLII), <http://canlii.ca/t/fpnld> retrieved on 2012-08-27

[4] Andrea Laing, "Managing the Rogue Employee," Corporate Risk Canada, Summer 2012, 10.

provinces. Most private enterprises operating in these provinces are governed by the privacy regulation specific to that province, with a few exceptions, including organizations under federal jurisdiction. There is other federal and provincial legislation that focuses specifically on the collection, use and disclosure of information in specific sectors, such as health care and financial institutions.[5]

Alberta is currently the only Canadian province with a broad breach notice law. (Ontario has one focused on health information only.) The Alberta breach notice law's primary notice obligation is to Alberta's Information and Privacy Commissioner, stating:

> *An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a **real risk of significant harm** to an individual as a result of the loss or unauthorized access or disclosure.*

In addition, organizations that suffer a breach may also have to provide notice to the impacted individuals:

> *Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner **may** require the organization to notify individuals to whom there is a **real risk of significant harm** as a result of the loss or unauthorized access or disclosure (a) in a form and manner prescribed by the regulations, and (b) within a time period determined by the Commissioner.*

Notably, the notice obligation applies only to those individuals to whom there is considered to be a "real risk of significant harm."[6]

It remains to be seen whether Alberta's notice requirement laws will be adopted by other provinces or at the federal level. In the U.S., breach notice laws passed in California sparked a push that led to breach notification laws now in place in some 46 states.

Proposed Changes to PIPEDA

The Federal government introduced Bill C-12, The Safeguarding Canadians' Personal Information Act, on Sept 29, 2011. This Bill reintroduces some of the amendments to PIPEDA that were first proposed in Bill C-29, which expired when parliament dissolved in March 2011. Most notably, Bill C-12 introduces requirements to notify people when there has been a breach of the security surrounding their personal information. Section 10.1 mandates reporting of "material breaches of security safeguards" to Canada's Information and Privacy Commissioner. Additionally, Section 10.2 under the Bill requires organizations to notify affected individuals if it is reasonable to believe there is a "real risk of significant harm to the individual." This bill is currently in the "first reading" stage. If passed, it will be interesting to see if there is an impact on privacy litigation. On a positive note, mandatory notifications can provide a valuable source of information regarding the nature of security breaches as well as the frequency and severity in which they occur. They can also be useful for evaluating the effectiveness of security measures currently in place.

[5] http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp
[6] http://www.infolawgroup.com/2010/05/articles/breach-notice/faq-on-albertas-new-breach-notice-law/

Cyber Risk Management as Good Corporate Governance

The U.S. Securities and Exchange Commission's ("SEC") division of Corporate Finance issued its first guidance on disclosing cyber security risks and incidents in October of 2011. It will be interesting to see if other regulatory agencies will follow suit. While not a mandatory requirement, the SEC's action is a clear indication to compliance officers and others in the business of corporate governance, both in the U.S. and Canada, that cyber security analysis, preparedness and monitoring is essential.

With the line between cyber security and regulatory enforcement becoming hazier for public companies, it is not a huge leap to consider board members themselves facing consequences, such as defense costs and possibly regulatory repercussions, from security breaches. At least two boards have already felt the sting of security-breach based derivative suits in the U.S.

As with other exposures, having an effective risk management strategy in place to manage cyber risks is essential.

A Time for Policymaking

As the stakes move higher and risk managers and board members work to actively manage new-age cyber risk, many are harking back to risk management fundamentals, namely policymaking. An effective cyber security policy is a company's first defense in protecting information, assets and people. Having a clear policy outlining permissible and impermissible uses of personal information and ensuring that the policy is both understood by employees and enforced by management is critical. Not only can this limit rogue employees' ability to abuse personal information, it can serve as evidence in the event of a claim that an employee's actions were not condoned and were prohibited by his or her employer, helping the employer potentially avoid future liability.

Since management is ultimately responsible for protecting the organization's information, it would follow that management must be closely involved in policymaking. Along with senior management, the team creating the cyber security policy and enforcing it should include representatives from multiple areas of an organization, including legal, human resources, information technology, operations and engineering/R&D/applications development.

According to Osler's Laing, companies should also clearly cover the issue of cyber security in employment contracts when an employee has access to sensitive information. This can further sever vicarious liability for the acts of rogue employees. "It is good practice to have counsel carefully review job functions and set data privacy practices and procedures for each role that handles sensitive information," she says.

The same team that drafts the network security policy should draft a detailed policy on how the company will respond to breach incidents that do occur. Such a plan is as essential as any other crisis management planning the company undertakes. When Sony Online Entertainment Network suffered a breach that affected millions of subscribers, consumers were not notified until several days later. One of the largest known attacks, it was also quite costly. The company's poor response will be remembered long after the bills are paid.

Bryan Thornton of Net Reaction LLC, an internationally recognized information security planning firm, provides the following points in a "Top 10 Guide" to effective information security.

1. **The board and senior management -- not IT -- have the ultimate responsibility to protect information**. In every lawsuit that has been filed over information security related issues, the board has been named. The board can delegate day-to-day responsibility for protecting information, but it retains the ultimate responsibility.

2. **Your information security program must include more than just IT**. While IT is important, there are several other areas such as trustworthy Human Resources, Asset Management and Incident Response that are out of IT's skill set. Neglect these areas, and your information will be just as unprotected as if you didn't have a firewall.

3. **Your program has to be holistic**. You cannot focus on one area to the exclusion of another. A good information security program must cover every aspect of a business.

4. **Information security is risk driven. Period.** Just as no two companies are the exactly same, no two information security programs will be exactly the same either. Your program must be driven by your specific risks.

5. **A good information security program includes everyone**. Ask around your organization. If only a couple of IT employees can explain what your company does to protect its information, then you don't have an information security program. To be effective, your program must include each and every person in the company, making them a part of your program.

6. **Information security extends beyond your borders**. Just as you must make your employees aware of what you are doing, you should also extend your program to include contractors, vendor and third-party providers. If they cause a breach of your company's data, your brand integrity and reputation will suffer.

7. **Communicate, educate and train. Repeat.** You cannot expect employees to reliably do anything that you do not explicitly train them to do. As such, it is critical that your organization communicates with employees and makes them an active part of an information security program.

8. **Be prepared to respond to incidents before they occur**. Organizations who are prepared to respond when an event occurs respond faster, with fewer financial losses and less damage to their brand integrity and reputation.

9. **Consider your policy on mobile and employee owned devices**. If it is important enough for them to take work home, it is important enough for you to provide a device from which they work. In most cases, there is no expectation of privacy on a corporately owned device.

10. **Never store what you can safely discard**. With the cost of restoring victims' identities in the case of identity theft continuing to rise, give thought to what data your organization is storing and then consider whether or not that data is really necessary. A lot of breaches could be prevented simply be appropriately disposing of data that is no longer in use.

Risk Transfer

Risk transfer is an important component of any risk mitigation strategy and insurance is an increasingly important strategy for cyber risks. Risk managers and board members need to be fully aware of the coverage available in the marketplace as it is constantly changing to adapt to evolving corporate needs. Because traditional insurance typically does not respond to data security and privacy events, boards need to be proactive in ensuring a comprehensive program to mitigate exposure. The approach should consider:

- Coverage for both first-party and third party costs associated with a breach incident.
- A broad definition of "covered information," encompassing not only the personal and private information of individuals but confidential corporate data.
- Coverage for legal liability damages and defense costs as well as regulatory actions, fines and penalties (as allowed by law).
- Coverage for the substantial costs a company will incur to manage an incident. This can range from computer forensics to get to the root of the problem, to coverage for notification costs. Even when provinces do not currently require notification, it can be good business to provide notice. A company's handling of an incident -- and support of those whose information has been compromised -- can go a long way in mitigating the reputational damage associated with an incident.
- Coverage that keeps pace with trending exposures, such as the risks arising out of an organization's use of cloud computing resources.

Board members and risk managers should evaluate cyber risk insurance not only as financial protection but as a way to ensure the prompt and expert response that is critical to mitigate damage to operations, finances and reputations in the event of a breach. In that vein, choosing an insurer with proven experience in this area is essential.

A Final Note

A robust corporate policy, with a toolkit that includes cyber coverage, should focus on identifying, managing, and mitigating cyber risk. Such a policy can give board members peace of mind that they have done their duty to avoid the legal liability, fines, penalties, and damages to the company's reputation that can come from something as simple as a misplaced USB drive.

##

Author:

Jeanette Lawrence, Assistant Vice President
Professional Liability, Canada
416 596 3943 Telephone
416 596 4068 Facsimile
jeanette.lawrence@chartisinsurance.com

CHARTIS
Your world, insured