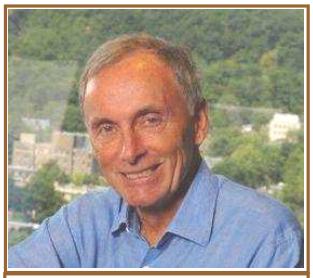
BFL
Makes a difference

Winter 2009

The Cover Note

EDITORIAL



Barry F. Lorenzetti

VOLUME 1, ISSUE 3
WINTER 2009

INSIDE THIS ISSUE:

During the past 20 years, our world has become entirely dependent on IT and the Internet, thus completely changing our lives as individuals and the face of the business world. I am quite sure none of us can imagine our lives without information technology anymore. Despite their many benefits, information technology advances have also produced their fair share of challenges and gave way to a new set of risks to be managed.

But have these risks been managed effectively so far? Every indication would lead us to believe that the answer to this question is no.

Many of us have received letters from companies advising us that personal information of ours was lost, misplaced or stolen. It also seems many incidents of systems breaches are hidden from the public in order to protect the reputation of the organizations experiencing these problems. Many systems have also been KO'd by viruses and other ailments! While some businesses still choose to ignore the risks, grabbing on to their favourite rabbit's foot – as if those risks could only materialize in other organizations – most companies who are trying to grapple with the problems rely on IT security experts who, often, are unfortunately oblivious of the business imperatives and regulatory issues at play.

Contrary to "bricks and mortar" exposures, cyber exposures are complex in nature as they encompass technology risks, people risks and business flow and administrative procedures risks. Therefore, managing them effectively requires a multidisciplinary approach as opposed to a lonely IT approach.

Furthermore, dealing with cyber risks requires bridging cultural gaps between different types of users. For example, it takes considerable efforts to get sales people to take cyber risks seriously and to accept and abide by security measures – the reason for this is simple: by nature and by assignment, they do not care for any rule or procedure which they perceive to be impediments to their sales activities and success; their focus on sales "blocking out" most any other type of consideration, even those concerning the company's overall best interest. Likewise, the IT or Finance personnel coming up with the rules are sometimes too removed from the sales activities to understand the impact of those rules.

This area of risk management is fascinating and deserving of more scrutiny and I would like to invite you to read on.

In addition, if you wish to read additional material about cyber risk management, I would recommend an excellent paper issued by ANSI (American National Standards Institute) and ISA (Internet Security Alliance) entitled *The financial impact of Cyber Risk: 50 questions every CFO should ask*. ♦

Cyber risk

John Wright, Executive Vice-President, BFL CANADA, Vancouver

During the last decade, the amount of personal data being stored by governments and businesses has grown exponentially and businesses have enabled access to information globally through supply chain integration and web-based commerce.

The frequency and severity of security breaches, system failures and data theft has increased at an alarming rate since 2006 around the world and industry leaders predict that data loss and theft will continue on this trend. Identity theft is the fastest growing crime in North America.

Industries that collect, store and use financial or health care data related to an individual such as financial institutions, retail, telecom companies, utilities, municipalities, insurance companies and medical associations are at most risk to identity theft.

The Potential Cost of Cyber Risk

The largest and most known privacy breach occurred when hackers stole customer information from at least 45.7 million credit card holders from TJX Cos. Ltd., the parent of Winners and Home Sense.

Outside experts predict the total cost of this breach could exceed $1 billion and direct losses could include business interruption from network downtime, costs to investigate, settlements with credit card companies to reimburse credit card holders, costs to defend class action law suits, costs to comply with provincial and state notification laws, regulatory penalties, costs to establish appropriate safeguards to their systems and procedures and public relations efforts to re-establish trust and goodwill.

These breaches could lead to both the company and Board facing lawsuits from customers and shareholders and other stakeholders. After a major breach the potential for the business to collapse as a result of a loss of reputation is the greatest risk to an enterprise unable to restore customer trust. Customers worry that their personal data provided online will automatically be at risk.

Surveys indicate that if customers do not believe a firm has the proper safeguards in place to protect their identities and personal data, they will not buy and will go elsewhere.

Cyber risk management requires businesses to have both effective preventive and responsive measures in place:

an effective information security safeguard policy and a privacy policy aligned with relevant laws.

Privacy legislation imposes clear duties upon all businesses, including non-profit entities and charities with respect to the acquisition, maintenance, and disposal of sensitive information.

Companies with third party service providers should ensure service agreements include clauses protecting the firm in the event of a loss or theft of personal information.

Cyber Insurance

Traditional insurance policies such as property, general liability, D&O, Crime and professional liabilities most likely include cyber insurance gaps. Most general liability policies for example have clear exclusions relating to cyber risk. These policies were not designed to envision the breach of security systems and the loss of personal data. In-house counsel and your broker should be asked to review both 3rd party service agreements and these traditional insurance policies.

Cyber Insurance is one of the fastest growing classes of insurance today. Earlier in the decade, insurers had difficulty establishing accurate pricing of this product due to the lack of meaningful actuarial loss data and case law. The result was a complicated application process, little consistency in the forms from one market to another and narrow insurance provisions. Clients took the position they did not need this expensive coverage and they believed a problem would not happen or could be easily fixed.

As the occurrence of losses increased and organizations began realizing the potential impact of cyber losses, demand for the product has increased. We have seen coverage expand, insurers ease the application process, increase limits and reduce pricing. Surveys indicate that Cyber insurance in North America increased by over 25% from 2006 to 2007 and 20% to 25% of companies now purchase cyber insurance.

Cyber insurance underwriting has matured and standard core coverages have emerged but policy wordings still vary substantially. Policies can be found that cover the cost of security breach notifications, public relations expenses and defense costs and penalties, with protection for information on the network, in mobile devices, and with outsourced service providers.

Insurer appetite does vary by industry. Careful analysis and customization remain essential in order to optimize Cyber Insurance protection at the best price.

Responding to a Major Cyber Breach

Organizations need to be prepared to respond to a significant Cyber breach with a formal Crisis Management Plan that is transparent, proactive, cooperative, and forms part of a larger plan to significantly improve systems security. Your organization must communicate its story before the media and blogosphere takes control.

Current and future stakeholders need to be assured, preferably by the CEO, that new controls are effectively in place, the problem will not reoccur, and your organization will deal with current

(Continued on page 3)

losses. The CEO needs to provide credible expression of concern, disappointment in the failure of its controls, apologize to all affected, and be committed to action. After a major breach, the objective is for all stakeholders to view your organization as a leader in protecting personal privacy now and for the future. ♦

Problems in the Server Room can Ripple Through to the Boardroom

Lyne Benoît, Senior Client Service Manager, BFL CANADA, Montreal

Bill Stoyles, Client Executive, BFL CANADA, Toronto

Taking on the role of director means personal liability and pressure from a myriad of risks. One of these often overlooked threats to directors and officers comes from cyberspace.

We have all read about cases of cyber problems in recent years. Many of those cases did not only involve fraud but also loss of personal information, libel, etc. and touched publicly traded or private companies as well as partnerships and non-profit organizations.

Claims under a Directors and Officers (D&O) policy can be triggered in a number of ways including:

- Breach of fiduciary duty, i.e., duty owed to bond and debenture holders or minority shareholders when applicable;
- Negligent management, i.e., not acting as a prudent person;
- Tort liability in common laws, i.e., the breach of a duty towards persons, primarily fixed by the law and which can bring an action for damages;
- Breach of Statutory duties such as those contained in the Competition Act, various Environmental Acts, and, most relevant to this article, PIPEDA.

Since directors face joint and several liability and in an increasingly litigious environment, the first "line of defence" in the protection of their organization and for themselves is to have sound risk management practices in place. This would include having a well communicated corporate-wide privacy policy, training procedures on privacy and data security, proper protection against hackers and e-vandalism, restricted access to systems and protection against copyright or trademark infringement. Having the audit committee review the organization's compliance with regulations and laws regarding the protection of privacy rights is also advisable.

A good risk financing and risk transfer program, including specialized insurance products, also comes into play to protect the assets of the organization. In addition to proper risk control measures, an effective way to protect the organization against claims resulting from cyber risk is of course cyber risk insurance – just as Directors and Officers Liability insurance offers protection for directors and officers against failure to perform their duties. (The original purpose of D&O insurance is to protect the individuals, not the company. Policies that protect both do exist, however, it should be noted that this leads to dilution of limits available for the directors and officers.)

With the tightening of laws and regulations concerning information technology, a greater strain could be placed on directors' liability and this should be one more reason for organizations to either purchase D&O insurance or review the scope of their existing coverage. It is essential to note that a D&O policy will NOT provide automatic coverage for cyber claims. Indeed, the wording of the allegations against Ds and Os will determine if the policy responds to provide defence costs and the nature of the alleged damages will need to fall under the scope of coverage or not be excluded. Furthermore, as mentioned above, the policy will not necessarily protect the company, by choice of either the Insurer or the Insureds.

It would be advisable for directors and officers to ensure the following points are taken into account in their D&O insurance policy to assist in protecting them, at least partially, against claims resulting from cyber risks:

- Removal of the professional services exclusion as cyber claims can often stem from performance of professional services;
- Removal of any clause imputing the knowledge of one insured onto another. This would help to offer protection to innocent parties that did not misrepresent on the application;
- World-wide jurisdiction – cyberspace knows no borders;
- Delete punitive exemplary damage exclusion;
- Priority of payments clause – if the policy covers both the directors and officers of the company, an endorsement stipulating that priority will go to the individuals over the company with respect to payments is a must.

In closing, we would stress the point that a D&O policy, no matter how well structured, only forms part of an overall risk management strategy and should be complemented with proper and targeted insurance coverages such as cyber risks insurance so that applicable coverage is there when it is most needed. ♦

ENHANCE YOUR RETIREMENT INCOME

Thomas Guay, President, BFL CANADA Consulting Services Inc., Montreal

Have you accumulated enough funds in your RRSP to provide an adequate income for the rest of your life? Based on current mortality tables, a 65-year-old male will live for another 19 years. A female will live another 22 years. It would take $900,000 at age 65 to generate a monthly income of $6,000 for the next 22 years on the assumption that that your portfolio will earn on average 6% per annum.

An Individual Pension Plan often referred to as an "IPP", can generate significant tax advantages beyond those provided by an RRSP. An IPP is a Defined Benefit Pension Plan just like many pension plans offered to employees of major corporations. It is a one-man plan, so all the assets belong to the plan member.

At age 50, the maximum current service contribution to an IPP is almost $6,000 higher than the maximum contribution to an RRSP. As you get closer to retirement, the cost to provide the benefit increases.

Your company can also fund past service benefits which could generate an additional tax deductible lump sum of approximately $150,000 that can be contributed to the plan. Added to this amount is the current service contribution of $26,000 for a total of $176,000.

The IPP is registered with the Canada Revenue Agency as well as with the provincial pension authorities depending on your province of residence. Upon establishing the plan and every three years thereafter, an actuarial valuation must be performed in order to establish the amount of allowable contributions for the next three-year period. If a surplus develops in the plan, it may be used to reduce ongoing contributions. Conversely, if there is a deficit, additional tax-deductible contributions are required to finance the deficit either in a lump sum or amortized over a period of 5 years. If your RRSP loses money, lost contribution room cannot be regained.

On retirement, the participant may purchase an annuity from an insurance company, have the pension paid out of the fund, or transfer the account value over to a Locked-In Retirement Account "LIRA" subject to prescribed limits.

In case of death prior to retirement, the full value of the fund may be rolled over to your spouse's RRSP on a tax-sheltered basis.

At death after retirement, if the participant chose a Life Income Fund "LIF", the remaining proceeds may be rolled over to the spouse's RRSP if he/she is under the age of 72 or to his/her RRIF, on a tax sheltered basis, if over age 71. If there is no spouse the proceeds will be payable to the designated beneficiary as taxable income.

Investments that are RRSP eligible generally qualify for an IPP and can be managed in a similar way as a self-directed RRSP. If funds are not on deposit with an insurance company, a trust is required. This may be a trust company or three individual trustees. Two may be related to the employer; however, the 3rd must be totally independent. All trustees must be Canadian residents.

It would be preferable and prudent to consult with an expert on this matter. We would be happy to answer any questions you may have. ♦

BFL CANADA
International Risk and Insurance Services

1-866-688-9888

BFL CANADA Risk and Insurance Inc.
2001 McGill College, Suite 2200
Montreal, QC H3A 1G1
Tel: (514) 843-3632
Fax: (514) 843-3842

45 Westwind Drive
Hammonds Plains, NS B3Z 1K6
Tel: (902) 864-4982
Fax: (902) 864-0200

2600 Laurier Blvd, Suite 840
Quebec City, QC G1V 4W2
Tel: (418) 658-6337
Fax: (418) 654-2045

1565 Carling Avenue, Suite 606
Ottawa, ON K1Z 8R1
Tel: (613) 722-7798
Fax: (613) 722-7829

BFL CANADA Risk and Insurance Services Inc.
181 University Ave, Suite 1605
Toronto, ON M5H 3M7
Tel: (416) 599-5530
Fax: (416) 599-5458

BFL CANADA Inc.
530 - 8th Avenue SW, Suite 1900
Calgary, AB T2P 3S8
Tel: (403) 451-4132
Fax: (403) 313-3365

BFL CANADA Insurance Services Inc.
1177 West Hastings Street, Suite 200
Vancouver, BC V6E 2K3
Tel: (604) 669-9600
Fax: (604) 683-9316

BFL CANADA Consulting Services Inc.
4115 Sherbrooke Street West, Suite 310
Montreal, QC H3Z 1K9
Tel: (514) 937-4188
Fax: (514) 937-5585

www.BFLCANADA.ca

For comments and suggestions, please contact:
Corporate Solutions
BFL CANADA
publications@BFLCANADA.ca