

CYBER RISK

Web-based technologies and extensive networks provide your firm's data users with convenient, easy and fast access to information. Your business may also have access to information globally through supply chain integration and Web-based commerce. On the other hand, your organization faces the possibility of large losses resulting from cyber risks, which can potentially destroy a firm's reputation through adverse publicity by eroding customer trust and goodwill, and significantly impairing shareholder value.

The frequency and severity of security breaches, system failures and data theft has increased at an alarming rate since 2006 in Canada, the USA and around the world, and industry leaders predict that data loss and theft will grow exponentially in the coming years. Identity theft is the fastest-growing crime in North America.

If your industry collects, stores and uses individual financial or healthcare data such as those used by financial and educational institutions, retail, telecom companies, utilities, municipalities, insurance companies and medical associations, then your firm is at high risk of identity theft.

The greatest cyber risk for your company is the potential for the business to collapse as a result of a loss of reputation should your firm be unable to immediately restore trust in your current and future customers in the event of a major breach of personal data.

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 are essential, as is an effective crisis management program.

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.



Cyber Insurance

Your traditional insurance policies such as property, general liability, Directors' and Officers' liability, crime and professional liability more than likely each contain cyber insurance gaps in them, which would not respond wholly or even partially to such losses. Most general liability policies, for example, have clear exclusions relating to cyber risk. These policies were not designed with breach of security systems and the subsequent loss of personal data in mind.

BFL CANADA's seasoned team of technology insurance specialists are experts in identifying these gaps as well as reviewing third-party service agreements for potential cyber risk problems.

If you believe you do not need this insurance or are under the impression that obtaining it is complicated, you should take another look. Over the past few years, Insurers have simplified their application forms and polished their products. Policies are now available to cover the cost of security breach notifications, privacy liability, crisis management, public relations expenses and regulatory defense costs and penalties, with protection for information on the network, in mobile devices, and some with outsourced service providers.

And, as breaches have increased, as evidenced by the regular reports in the media about such incidents, the purchase of cyber risk coverage has grown significantly. It is believed that in North America approximately 30% of companies now purchase cyber insurance and this number is growing every day.

BFL CANADA technology professionals are knowledgeable, innovative and responsive; they will guide you through changing industry requirements, emerging coverages, new insurers and evolving underwriting requirements, as well as provide a variety of different solutions to meet your specific needs.

