Gallagher
Insurance | Risk Management | Consulting

100 Scurfield Blvd.
Winnipeg, MB R3Y 1G4
Canada

204-925-8550
www.ajg.com

The Evolution of Cyber Exposures & Risk Transfer Solutions
by Brian Dagg, Gallagher Insurance

As the world becomes more data-driven and interconnected, and our reliance on technology increases in the day-to-day function of both our personal and business lives, our exposure to a cyber-attack impacting the operations of our business also increases.

The risk of a cyber-attack extends to organizations of every size around the globe. Whether we are a publically traded entity, a privately held company or a not-for-profit organization, we are exposed to the risk of a network attack. From a breach of personal information that has been entrusted into our care, to a ransomware attack locking us out of our systems and causing a loss of business income, to a social engineering or phishing attack causing the loss of money, the exposures continue to evolve.

When does liability arise?

Examples of potential exposures include breaches of personally identifiable information, including names and addresses, or email addresses, financial information, health information, corporate confidential information, virus transmission, data loss, and cyber extortion, among others.

In Canada, legislation has recently changed with respect to privacy. As of November 1, 2018, organizations now have the obligation to notify individuals in the event a breach if they face the risk of "significant harm". Something as simple as an email address may constitute the risk of "significant harm" under the new legislation due to the exposure that individual may face due to phishing attacks. Reporting must also be completed to the Privacy Commissioner of Canada, and records must be kept pertaining to all breaches of personal information, whether or not notification may be required. Failure to meet your obligations under the new legislation may result in regulatory fines up to $100,000. With the new legislation, it is imperative for organizations to review their internal procedures surrounding the storage of data, data retention policies, and data destruction policies, determining what is reasonable. If a client utilized our services eight years ago and they have not returned, is it reasonable for us to maintain their information within our networks?

Why is cyber insurance so important?

Data is one of your businesses most important assets, and data related incidents are generally excluded from your property and casualty business insurance policies.

A data breach may result from one of several scenarios – a malicious cyber-attack by a third party targeted to your organization or received at random, the loss of paper files, the improper disposal of information, accessing unauthorized information within the network by a rogue employee, the use of cloud based services without an adequate back-up system, network failures, and more.

Not all privacy breaches are driven by criminals. More than one third of all breaches are either intentionally or accidentally caused by employees.

A breach may cause far-reaching damage, extending beyond direct financial loss, including financial, reputational, legal and regulatory damages. Depending on the jurisdictions in which you transact business, your obligations may vary – privacy laws in the United States vary from state to state, the new General Data Protection Regulation (GDPR) in the EU has the ability to impose significant fines and penalties in the event of a breach involving the data of EU citizens. Legislation applies in the jurisdiction where your client resides, and not where your business is located.

What protection does cyber insurance provide?

In today's competitive marketplace, cyber insurance policies can be very broad, covering a long list of first and third party exposures to your business and to third parties you may interact with. Generally speaking, cyber insurance is coverage designed to specifically respond to the financial impact of an event. From the provision of expert forensic IT and breach counsel resources, to the defence and settlement of a suit alleging a breach of privacy, network security or media liability, the handling of an extortion event, including the acquisition of cryptocurrency, the loss of business income, and out-of-pocket costs incurred in handling a network attack. The importance of having experts in the cyber world to look after your interests when responding to an attack cannot be overstated.

Many insurance carriers are unveiling new products to address cyber risk in different capacities – from extensions of your property and liability policy offering, usually, a limited form of coverage, to stand-alone policies offering comprehensive, robust coverage. With that however, no two policies are the same – coverage, sub-limits, extensions or limitations vary greatly from carrier to carrier.

The term "cyber" implies protection for incidents the involve electronic hacking or online activities, however the coverage is much broader, and also provides coverage for personal or confidential information and communications in many different formats – paper, digital or otherwise.

While cyber insurance is intended to protect the loss of data, policies may be broadened to cover electronic theft and the element of social engineering fraud (being duped by a fraudulent source purporting to be a colleague, superior or trusted vendor to transfer funds electronically).

Ultimately, all businesses are unique and your exposures may vary, however in all instances, data is an important asset and must be secured. There is no substitute for a sound cyber-security strategy, effective systems, processes and training that keep your data and systems as safe as possible. Even with the best physical protections, any organization relying on technology and the safe processing and storage of data is best served by having cyber insurance to augment their cyber-security strategies.

Cyber risks are increasing with new trends emerging all the time, and unfortunately, this is the new world in which we live. What worked for us last week, or last year would be fine, if it was last week, or last year. Today, the rules are different, they are changing and the problems we encounter are more complex than ever. Cyber-security needs to be viewed as an investment, and not an expense. That investment is more than just financial – it is a cultural investment in doing your part to ensure the protection of the personal and confidential information we are entrusted with. Cyber-security is about the people, the process and the technology – without one of those three, cyber-security becomes largely ineffective.

About Gallagher's Management Liability Practice

Gallagher's Management Liability Practice in Canada consists of professionals dedicated to protecting individuals and their organizations against an array of executive and professional liabilities. We have a firm understanding of where standard policies leave off, when cyber insurance is most effective, and the statutes and regulations surrounding the ever increasing regulatory requirements.