Cyber Liability

Amanda Dean, BPR, MBA
Atlantic Vice-President,
Insurance Bureau of Canada

Cyber liability received front-page attention last November when hackers stole and released data from the systems of Sony Pictures in protest over the company's new movie The Interview.

Other, less famous, cases of recent years include:

• The loss of a thumb drive containing personal information by an Ontario nurse, costing her employer $500,000.

• A Canadian bank forced to compensate customers when personal information was accidentally faxed to unauthorized third parties.

• A car company being the subject of a class action lawsuit over a hard drive that went missing.

Other than Sony Pictures, all of these events occurred in Canada. And there are others. The lesson is that cyber risk is growing and takes many forms, and that no organization – big or small – is immune.

As with any emerging risk, cyber liability presents both an opportunity and a challenge for insurance companies and their broker partners.

Is your brokerage ahead of the curve? Do you have the expertise to offer advice and solutions to your commercial clients? Also, what about your own business? Do you know your risks and are you protected?

Cyber insurance is one of the fastest growing areas of insurance, both in terms of availability and uptake. It has evolved a fair bit over the past couple of decades. In the 1990s, court decisions found that cyber risks were covered under a CGL policy. In response, insurers began excluding liability in respect of electronic data, opening the door for cyber coverage to be available as a stand-alone policy or an endorsement.

Initially, the product was mostly for large, sophisticated clients, but over the years standardized policies suitable for small and mid-sized organizations have been developed. Currently, about 30 insurers sell it.

It varies by policy, but coverage can include costs for:

- Notifying customers in the event of a breach
- Hiring a computer forensic investigator to determine precisely what data were lost or damaged
- Credit monitoring services
- Hiring a privacy lawyer
- Crisis management
- Regulatory fines
- Loss of business income

The move towards mandatory breach reporting plays a significant role. This is more advanced south of the border, where there are 46 states that have mandatory breach reporting laws. As you'd expect, wherever such laws exist, class action lawsuits increase.

Here in Canada, Alberta is the only province with its own breach reporting laws, but it's safe to assume the rest of the country will follow suit. When that happens, expect a sharp spike in interest in cyber insurance from commercial clients large and small.

We're all still learning about this emerging risk. In a recent news report, Robert Hartwig, President of the Insurance Information Institute said: "This is like insuring aircraft in 1915—there's a lot more we don't know than we do at this point. And I think part of this involves developing expertise, developing databases that help us understand the nature of these attacks."

As we go through this learning process, brokers are on the front lines, handling questions from commercial clients with (understandably) rising concerns and interest in what our industry can offer them. Forward thinking brokerages are already building their knowledge so they can offer tailored solutions to meet their clients' needs.

At the same time, it's important to make sure your own shop is protected.

Financial businesses, being in possession of personal and sensitive information, are especially vulnerable; even more so if you use e-commerce as a method of distribution, or if you have employees who carry around devices that could contain sensitive information.

The potential costs also include reputational damage. A study by the Canadian Privacy Commissioner found that 71% of Canadians believe that protection of personal information will be one of the most important issues facing Canadians in the next 10 years, and 97% said they want to be informed in the event of a breach. In other words, customers expect privacy and have low tolerance for those who fail to deliver.

There are a number of things you can do to protect your business: the use of encryption on mobile storage devices, employee training, assigning someone in the office to be in charge of cyber protection, etc.

A critical first step is knowing your risks. To this end, the Office of the Superintendent of Financial Institutions has developed a useful tool: the Cyber Security Self-Assessment Guide. It's voluntary, designed with federally-registered financial institutions in mind, but it can be used by any business as a starting point to evaluate existing risks and the quality of protections currently in place.

Consider using OSFI's guide yourself. Also, consider recommending it to your clients.

Whether or not you use the OSFI guide as your starting point, it's important to be proactive on this issue. Cyber liability is only going to grow, as a risk and as an opportunity. The smart move is to act now to ensure your business does not suffer the costly consequences of a breach, and, at the same time, to take advantage of this rapidly growing area of our business. ■

Amanda may be reached at (902) 429-2730 ext. 225 or via email at, adean@ibc.ca.