cloud managed networks

Cyber Insurance – One Size Does NOT Fit All

By Jane-Michèle Clark
October 8, 2020

Business owners, executives and IT specialists have come to accept that a data breach is truly not a matter of "if but when", to quote that all-to-often used phrase. Much has been written on how to protect a firm's network, devices and data, but managers are less certain about how to choose the right cyber insurance coverage.

Despite knowing the huge impact a data breach has on business operations and the bottom line, many organisations prioritize obtaining coverage for bricks and mortar over data and related assets. That can be a mistake. A big one.

The importance of having good cyber insurance in place was stressed in multiple sessions in the October 2020 Virtual conference on Keeping Pace with Cyber Security in Ontario's public sector. Ditto in several other cyber security conferences, hosted by myriad industries, attended over the past year.

A common theme from executives whose organisations had fallen victim to some form of cyber crime: *"Knowing what I know now, I would make my insurance decisions differently today."*

Some simply said: *" I would make sure we had proper coverage!"*

Costs of a Data Breach

Depending on whose report you read, you'll get different figures. Indeed, we have used different ones from time to time.

Poneman Institute 2019 research suggests that a single stolen laptop, even if password-protected, can cost business on average $39,000 USD, if it contains confidential data. The figure is higher if there are automatic ways to access the corporate network., or ways to access the network.

According to the Insurance Bureau of Canada*:

- Canadian cyber crime costs total approximately $3 Billion a year which is 0.17% of the Canadian Gross Domestic Product (GDP).
- In 2018, the average cost to detect and contain a data breach, including crisis management, is approximately $1.78 Million.

**www.IBC.ca*

Nearly 60% of Canadian SMEs , and at least 25% of enterprise-level firms, do not have adequate cyber-related crime and data breach insurance in place. Many these believe the "cyber" portion of their commercial insurance has them covered. Not so.

According to Mark Lefebvre, Insurance Bureau of Canada, many firms feel secure with what is really a cyber "light" (as in light/lite beer) package, mostly because this is a relatively new and continually evolving area – for both the insured and the insuring companies. He says, *"There are many different flavours of coverage, that a lot of providers are couching as 'cyber', but you must ask: 'What is cyber?'".*

Many executives believe that if the data breach, or the network shutdown is a result of something that happened with a laptop, computer, or other electronic device, that it counts as a cyber incident. Insurance companies think differently. This becomes readily apparent when you go policy shopping.

There are separate policies and coverage levels for:

Phishing. 99% of malware and ransomware is delivered through employee emails.

Social Engineering. Yes; this is viewed as distinct from cyber hacking and stealing of data. Although some social engineering can be connected to phishing, this can also include multi-step attacks.

For example, by accessing a company's org chart, and obtaining a specific executive's cell phone number (possibly through a phishing approach), the stage has been set for crime to occur. The criminal spoofs the cell phone number and contacts a mid-level finance department employee. In a large firm, the finance person likely does not know the executive's voice, but *does* know the name and title.

So… when the "executive" says that a key supplier's banking details have changed, the dutiful employee may be all too ready to help change the information over the phone. Or the imposter claims to be the CEO, saying that a small competitor is being acquired and that funds need to be transferred, and that the lawyers will be sending an email shortly to confirm the request and provide the banking details. The pseudo-CEO adds that the employee's discretion must be counted on because this sale is not yet in the public domain. Shortly thereafter, the "lawyer's" email arrives and the funds get transferred. These scenarios sound far-fetched, but they do happen, and more often than you might imagine.

Electronic Funds Transfer "Errors". This can be a result of cybercriminals or employees taking on the role of bad actors. There has been an increase in this type of fraud since the pandemic began. Companies that previously required two signatures on a major amount cheque are now routinely transferring funds chronically, and this makes them more vulnerable.

Denial of Service, Spoofing, Malware and Ransomware.

Business Interruption.

Notifications, Reporting, Media and Other Communications.

Loss of Reputation - though it can take years for the impact of a reputation hit to be reflected on the bottom line.

Directors and Officers Insurance. Increasingly senior executives and board members know they can be held liable, so many firms need to consider D&O coverage as part of their cyber protection approach.

Not usually covered: Fines

According to the Insurance Bureau of Canada, there is no company that will pay the fines levied by government or stakeholders. That said, it's an evolving industry and you need to do your due diligence.

Although fines are rarely paid, the costs associated with the related negligence (e.g. person's private data is used to obtain a fraudulent loan), is covered by some policies.

Although all businesses today require some level of "cyber" protection, not all face the same level or type of risk.

The type of work you do, the industry in which you operate, the size of your workforce and the degree to which they operate remotely, the number and locations of your branch offices, the number of outside stakeholders that need to connect to your network, the number of personal records you retain and the degree of personal information that is part of those records, the number and types of platforms and applications your company uses all determine the level and type of coverage you will need.

How can you ensure you have the right coverage for you?

1. Gather a team that includes key C-Suite executives, your legal representation (internal and/or external), IT and network specialists (again, internal and/or external, as appropriate), operations managers and the finance department.

   You need to include key members from the finance department, including the CFO, because they are the only ones able to properly quantify the loss before it happens. Too frequently, companies underestimate the cost of notifying people in the event of a breach, and the financial impact of every hour of "business" downtime– and without realistic figures, it's almost impossible to choose the correct amount of insurance required.

   The other team members are needed to help determine how your company will respond in the event of a breach. How you plan to respond, and what you are required to report depending on the types of records you hold in the industry in which you operate, will also impact the cost of a breach.

   A key loss cost variable: The number of records your firm retains that contain personal data or private commercial data.

   Armed with this information, you are now ready to consult the top cyber insurance specialists in your region. How can you find them? Not by Googling "cyber insurance carriers".

2. Lefebvre says, *"We're in the days of the Wild West when it comes to cyber insurance. US insurance is very different terms of contract language than insurance providers from the UK – and Canada is influenced by both."*

   So, talk to your commercial insurance provider and ask for the names of two cyber insurance specialist firms. Talk to a few CEOs in organisations similar in size and industry to yours and get three names from each of them. Then, make an appointment with your commercial insurance provider and the two names that were common to the most lists and do your due diligence. Some questions to discuss with prospective carrier candidates:

   - What is your definition of "cyber crime" and how is that differentiated from data loss and data theft?
   - Do you cover fines? What about negligence-related damages?
   - Are cyber extortion, ransomware, social engineering, data breach remediation, data recovery, crisis management, notifications, media relations, business interruption and other related expenses covered by separate policies – or are they all part of a single offering?
   - Are manuscripted policies possible?

- How often is a security vulnerability assessment and/or penetration testing required for the insurance to remain in place?
- What kind of logs need to be retained – and for what period of time?
- What are your reporting requirements? What about release of confidential client data? The latter is important if some of the data you retain is protected by client-solicitor privilege.
- Is it possible to make a claim as a result of an intrusion that is not detected until several months or years down the road? If so, what is the time limit?
- What security applications can you deploy, and/or protocols can you implement, to reduce your premium and deductible costs?
- Do portable media and computers need to be encrypted?
- What about encrypted data that is controlled by third-party service providers?

This is not an exhaustive list, but intended to give you an idea of topics to bring up when choosing a carrier. Regardless of your organisation's size, it is important to select a firm with longevity and a solid reputation.

In one of the cyber security conferences, a CIO asked, "*We recently got turned down for cyber security coverage by our current carrier. We are currently looking for new provider, but what should we do?"*

Ensuring Your Firm Remains Eligible for Coverage

Every year, commercial insurance carriers require their clients to complete application forms that include a detailed "cyber" application form. All IT enhancements must be noted, including network upgrades and patches. Today, insurance companies want assurance that your system is well-protected from edge to endpoint.

Given that relatively few breaches occur as a result of a brute force attack, an insurer's employee access protocols and training standards and frequency can be requested, too. According to Lefebvre, a Chubb underwriter and two CIOs whose systems were recently held for ransom: An insurance underwriter may not be willing or able to quote on a business if it fails to refresh and update its network, and/or does not have adequate security software in place from edge to endpoint, and/or fails to upgrade its system regularly or push the patches out to all endpoints.

So, to answer the *"What should we do?"* query:

Bring in a third-party expert to do a vulnerability assessment, update your systems, train your employees according to the recommendations – and stay on top of things.

For more information, please go to Public Safety Canada (https://www.publicsafety.gc.ca) where you can find various cyber crime reports and prevention guidelines.

You are also welcome to contact us: **Cloud Managed Networks**, www.cloudmanged.ca, 1.877.238.9944.