SELLING CYBER RISK

STAND-ALONE CYBER RISK INFO FOR BROKERS



USE FOR BROKER EDUCATION ONLY

Provided by, Forward Insurance Managers Ltd.

Forward
PEOPLE + TECHNOLOGY

WHO NEEDS CYBER INSURANCE?

As more businesses transform digitally and cyber crime becomes more prevalent, all business owners should be looking closer at how they protect customer data, their corporate networks and their trusted reputations.

Many owners may not fully understand the extent of customer data their systems capture, how that data is secured and the potential liability they may incur should they suffer a cyber attack.

Businesses need to consider a stand-alone cyber insurance policy if they,

- Process and store sensitive customer or patient data
- Provide computer software or hardware services
- Use point-of-sale systems

KEY INDUSTRIES

Retail / Wholesale / Ecommerce / Health Care / Information Technology / Financial

TALKING POINTS

- Cyber attacks can be expensive and many businesses may go out of business after suffering a cyber attack.
- Is your network protected by a business grade firewall and antivirus?
- Is all critical data backed-up to a completely separate location from the business network?
- Do you password protect all portable media including smartphones and memory sticks?
- Do you have trained personnel in place to prevent attacks?

Forward
PEOPLE + TECHNOLOGY

MY CURRENT POLICY COVERS IT ?

Many business owners may think that their standard liability policies are sufficient to cover cyber risks, but in many cases the wordings in these policies are not explicit enough to provide adequate (if any) cyber coverage.

TALKING POINTS

- Bundled standard policies are likely not designed to protect against today's fast moving cyber risk landscape.
- Cyber risk is similar to other challenging specialty lines such as Directors & Officers (D&O) and Employment Practices (EPLI) coverages.
- Increased frequency and severity of events make it difficult to address cyber coverage in a generic multiperil policy.
- Standard policies can sometimes result in claims disputes over "silent" coverage (when cyber isn't explicitly named, but isn't specifically excluded).
- Higher coverage limits may be easier to come by in stand-alone policies.
- Caution about "trapdoors" and "landmines" that may exist in standard policies which could leave companies exposed if affirmative coverage has not been negotiated with clear terms and limits.

NO BUSINESS IS TOO SMALL

According to a 2019 StatCan report, one-fifth of Canadian business were targeted by hackers. Small businesses may be targeted by hackers because they often don't have secured infrastructure or expensive personnel dedicated to preventing attacks.

Many Canadian businesses use anti-malware software, email security and network security to protect their information and communication technologies infrastructure. However, a lack of usage of other cyber security techniques may still result in businesses being vulnerable to cyber security incidents.

Reference: https://www150.statcan.gc.ca/n1/daily-quotidien/201020/dq201020a-eng.htm

TALKING POINTS

- Small businesses may be seen as low hanging fruit for hackers.
- Many small businesses don't mitigate the risk until after an event.
- Specially trained cyber security personnel can be costly for small businesses.
- Stand-alone insurance is a cost effective solution for small business.
- How would you handle a cyber breach?
- Do you have a plan for customer notification post-hacking event?
- Be proactive, not reactive with cyber protection and your corporate reputation.

COSTS, COVERAGE AND CLAIMS

Cost of coverage, extent of coverage and an unsatisfactory claims experience are all top reasons why many companies do not have stand-alone cyber risk coverage.

TALKING POINTS

- Purchasing a cyber risk policy can be relatively cost effective.
- Stand-alone policies provide more adequate coverage, with clear terms and limits.
- Higher coverage limits may be available with a stand-alone policy.
- Caution about "trapdoors" and "landmines" that may exist in standard policies which could leave companies exposed if affirmative coverage has not been negotiated with clear terms and limits.
- Be proactive, not reactive with cyber protection and your corporate reputation.
- We've partnered with Avast antivirus and malware software providers to help you protect your critical networks. You'll receive business grade antivirus and malware protection with your policy.
- We are committed to quality claims service. We know it can be stressful when an incident occurs and we'll be here to assist.

SELLING STAND-ALONE CYBER RISK IS ABOUT GREATER AWARENESS

Policy holders and brokers alike require greater awareness to navigate the rapidly changing landscape of Cyber Risk. Forward Insurance Managers Ltd. is committed to being your partner in awareness and helping to insure the future of business Cyber Risk.

For more information visit our website
https://forwardinsurance.ca

Forward
PEOPLE + TECHNOLOGY