RISKPOINT
INSURANCE ADVISORS

Cyber Liability, Crime & Advertising Injury

What does it mean?

Recently there have been a lot of questions surrounding Cyber coverage and confusion about three areas of insurance coverage and exposures: Crime, Cyber Liability and Personal/Advertising Liability. The article below will bring clarity to the separate areas of coverage.

It is our recommendation that each exposure needs to be evaluated and insured separately. Just because you buy coverage doesn't mean it will cover what you expect. Make sure you understand what you are buying and if it fits your company's exposures as well as your expectations.

CRIME COVERAGE

Cyber coverage should not be confused with "crime coverage." Crime coverage provides the client with coverage from the theft of money, securities or property either from a dishonest action of an employee or a third party. This can be the result of physical theft (employee taking money from a till), fraudulent check writing, or a third party manipulation of their computer system to steal money or fraudulent electronic transfer (EFTS).

A crime policy will not respond to any claim arising out of the theft of information, only money, securities or property. A crime policy pays the client directly if these are stolen, or in the case with customer property in the client's care, custody or control, it reimburses the client for the theft so they can make their client's whole, if customer property coverage is purchased.

RISKPOINT
INSURANCE ADVISORS

Crime policies do not cover "voluntary parting of money." So if an individual or customer innocently makes an online payment or an EFTS transaction to a criminal (normally as part of a phishing attack), the policy will not respond. However, just recently, several insurance carriers have started offering what is termed as "social engineering coverage," which provides a sublimit of coverage for clients that pay out money to criminals who have misrepresented themselves as customers or legitimate business entities.

CYBER LIABILITY

Cyber Liability claims arise out of either a privacy violation (failure to prevent unauthorized disclosure such as losing a laptop or misdirected emails) or from a failure of network security, which allows a hacker to steal confidential data (not money) such as personal identifiable information, patient healthcare information or corporate confidential data (business plans, financial statements, formulas, bidding information). The latter is a result of criminal activity and does not cover the direct theft of money, only information. This is where the confusion comes in as the theft of data may be called cyber crime, but the crime involves stealing information. The criminals steal the information to commit fraud, such as creating bogus credit cards or initiating fraudulent EFTS transactions by misrepresenting themselves as the customer to a financial institution. A cyber policy will defend an insured if sued by a third party but only if such a claim arises out of the theft of the third party's personal identifiable information or corporate confidential information that was in the insured's care custody or control or a third party for whom the insured is legally liable. Cyber policies however, do not cover identity theft when a criminal creates a fictitious email using the insured's email address to send a fraudulent email to a customer to induce them to send money. In this situation, there has been no theft of information, the criminal is simply taking advantage of the insured's identity to trick a third party to send them money.

"Make sure you understand what you are buying and if it fits your company's exposures as well as your expectations."

To fully protect themselves, clients need to buy both a cyber policy and a crime policy. The cyber policy will provide the following (assuming all options are selected): Third party liability, including coverage for regulatory claims, including fines and penalties. PCI coverage for claims filed by merchant banks after a data breach in which it is found that at the time of the breach the insured was not PCI data security compliant. Coverage will include the cost of defense, forensic investigation expense, fines/penalties, fraud assessments and cost of reissuing cards, all of which the insured is contractually liable for if not PCI data security compliant at the time of a breach.

RISKPOINT
INSURANCE ADVISORS

First Party coverage includes:

- Notification/credit monitoring costs
- Forensic investigation expense
- Cyber extortion (ransom payments if information is stolen and there is a threat to disclose or if the insured's network is subject to a denial of service threat)
- Data restoration expense (costs to recreate damaged or destroyed electronic records)
- Cyber Business Interruption
- Cyber Reputational Harm (Loss of income once computer system is back up and running but breach has become public and as a result, there is a loss of customer activity)
- Public relations expense

PERSONAL AND ADVERTISING INJURY

When an injury to a third-party occurs as a result of a business advertising its products and services, it is labeled a personal and advertising injury. The injury can occur as a result of trademark or copyright infringement, slander, libel, defamation or invasion of privacy. For example, a competitor of your small business complains an advertisement, act, comment, blog post, or practice you or an employee made has damaged their business. In another personal and advertising injury example, an advertisement you are marketing makes a false claim about your competitor's products or services.

When a competitor has suffered damage to its business as a result of an advertising injury, the competitor may decide to sue your small business for a specific claim, such as trademark infringement, copyright infringement, defamation, libel, slander, misappropriation of advertising claims, etc. A personal and advertising injury insurance policy is a type of general liability business insurance to provide protection against this type of claim.

In the case with all three exposures and the coverages that protect you and your company, it is important to address each of these individually. A common misconception is because losses or claims occur electronically, a cyber liability policy will cover all electronic or "cyber" losses. Consult with a broker who has expertise in these areas and isn't just selling you a policy as all policies are not created equally. Ensure that when you do purchase coverage, you know what you are purchasing and it fits your company's exposures. Just as you evaluate your property and other liability exposures annually, it is our recommendation every company include these three areas of exposure in your annual insurance review process.

For more information please contact:

Blake Schellenberg
President
5285 Meadows Rd. Suite 242
Lake Oswego, OR 97035
Phone: (971) 282-4317 I Email: brs@riskpointins.com