A FOCUS ON CYBER CLAIMS

Cyber insurance will provide coverage for an insured's 1st Party and 3rd Party losses associated with network security breaches or the loss, theft or unauthorized disclosure of Personally Identifiable Information (PII) or confidential corporate information. This coverage could include expenses related to breach notification, extortion threats, public relations, credit monitoring, forensic investigation, defence costs and the costs of judgments or settlements.

Every business, regardless of size or industry, has an exposure and should be protected accordingly. Exposures come in the form of employee information, customer information, internet access, electronic and network activities and the overall use of technology.

The Case of the Missing Laptop

An employee at a small accounting firm took home her office laptop to do some work over the weekend. But an ill-fated stop at the mall left her with a broken car window, a stolen laptop and exposed more than 120,000 people's personal records. Her firm had been helping several large hospitals with their audits, and their patients' protected health information (PHI, which includes prescriptions, procedures and diagnostic codes) was now a password away from the thieves. Our response team was able to advise the firm on how to notify each hospital and then each patient. The firm was able to stay in business.

Employee Data Posted to Company Website

A publicly traded company became a little too public when it unwittingly posted the personal information of several top executives online. Social Insurance Numbers of the company's top brass were accessible to anyone who visited the company's website for four to six weeks. The in-house legal department contacted Trisura's panel of experts about the breach. Those firms made two key recommendations: Investigate the weblogs of online visitors during that time and determine whether search engines had indexed the information. The extent of the breach turned out to be minimal. The search engines had not indexed the data, and it was housed on a part of the site that was seldom visited. Because of the executives' high-profile, however, several precautions were advised and taken: The company put a fraud alert on all bank accounts; conducted a credit file activity review; and put all individuals on the highest level of credit and fraud monitoring.

IT Oversight Leads to Breach

When a police department updated its databases, critical information was placed on a standard, non-secure server. The personal information of more than 200,000 officers, prisoners and informants was exposed for eight months due to IT oversight until someone voiced a concern about the personal data appearing on search engines. The police department contacted Trisura's panel of experts to determine whether it should consider fraud remediation. The team took into account several factors, including the large number of individuals exposed and whether the department could be sued. The department decided to respond to specific safety concerns rather than launch a consumer-based protection campaign. Monitoring and fraud resolution were determined impractical.

The Wrong Kind of Credit Card Slip

A small online merchant was in the process of transferring its data and redesigned website to a new host when the old website was hacked. The potential thieves gained access to nearly 30,000 credit card numbers dating back nearly five years. Even though it is illegal to hold onto these numbers so long after the transaction, the merchant still needed to inform its customers of the breach. The breach response team suggested that the merchant filter out all the credit card numbers that were still active, which reduced the affected group to 12,000.

Then, the response team worked with the merchant's legal counsel to determine if it was worth informing the group (it was), provided a notification letter and FAQ template, and access to our cyber response team experts where customers could get advice on further protecting themselves. The response team also helped the merchant prepare for litigation against the host who caused the breach in the first place.

Policyholder Data Stolen

An agent left an insurance company for another and, using his former colleague's login credentials, stole thousands of clients' names and personal information. He then called these clients and quoted them better rates for their homeowners, health and auto insurance. Trisura's cyber response team came in to handle the situation after the insurance company immediately filed criminal and civil charges against the former employee. What was the assessed risk to policyholders whose personal information had been stolen? Not high and certainly not high enough to risk the scrutiny of the court and regulators. The response team advised how to monitor the breach considering the low threat and how to recover costs as damages in the civil lawsuit against the former agent.

Mortgage Applications Go Missing

A credit union reached out for assistance after a third party vendor lost a number of closed mortgage applications. The credit union was legally required to keep the closed mortgage applications. It hired a storage vendor that reported a missing carton containing 14 closed mortgage applications. The vendor searched its facility but nothing turned up. Trisura's cyber breach response team worked with the credit union's general counsel to draft a letter notifying the consumers without causing panic, then helped the recipients enroll in services that would ensure their information wasn't misused. The storage vendor also came through by covering the costs spent on notification and monitoring.

Leased Photocopier Leads to Breach

A news organization bought a photocopier that had once been leased to an insurance company. The media group's investigative reporter discovered that the copier's internal hard drive still contained all the information that had been copied by the insurer. The journalist contacted the insurer because it was planning a news segment about the data risks copiers pose to protecting sensitive personal information. Trisura's cyber breach response team worked with the insurance client to determine what information had been leaked and provide a notification letter template. It referred the client to a special PR firm to handle the on-camera interview for the news segment. The resulting televised story was very respectful, did not single out or attack the client, and regulators decided not to take action based on the facts presented.

About Trisura

Trisura Guarantee Insurance Company is a Canadian specialty lines insurance and surety company. Through a select network of national and regional brokerage firms, Trisura Guarantee provides innovative solutions and expertise in Contract, Developer and Commercial Surety, Directors' and Officers' Liability, Fidelity, Professional Liability including Media, Technology and Cyber Liability, Property, Casualty and Warranty products. Trisura Guarantee is rated A- (Excellent) by A.M. Best Company.

Trisura Guarantee is a subsidiary of Trisura Group Ltd., a leading international specialty insurance provider operating in the surety, risk solutions, corporate insurance and reinsurance segments of the market. Trisura Group has three principal regulated subsidiaries: Trisura Guarantee Insurance Company, Trisura International Insurance Ltd. and Trisura Specialty Insurance Company. Trisura Group is listed on the Toronto Stock Exchange under the symbol "TSU".

For more information and to download our application forms please visit our website at www.trisura.com

Refer to your policy for complete details. In case of inconsistency between this document and your policy, the policy terms, conditions and limitations will apply.