Cyber Privacy Protection

By Red River Mutual

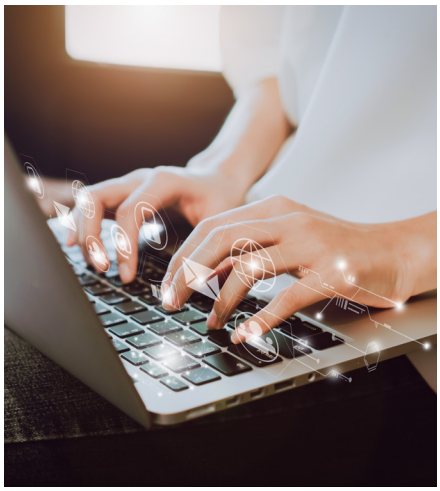
Why Upgrade Your Cyber Privacy Protection Coverage?

We know that privacy breaches are occuring with alarming frequency – in Canada, and worldwide. As a business owner, what you're less sure of is how to deal with a breach when you suspect one has occured. That's when you call in the experts. Our upgraded **Privacy Breach, Cyber Event Recovery and Cyber Event Liability** coverage will help protect you against Data Ransom, Extortion and Blackmail, not to mention Regulatory Fines and Penalties.

This optional coverage is available at an additional cost for Red River Mutual's Commercial policyholders who want to increase their First Party and add Third Party liability coverage in the event of a privacy breach.

WHAT YOU'RE GETTING:

The piece of mind knowing that you have an experienced CyberScout Breach Response Expert on hand to walk you through an investigation and advise you on how to protect your business. Still unsure if you should upgrade your covereage? Take a look at a few breach ***Case Studies***, courtesy of our partners at CyberScout.

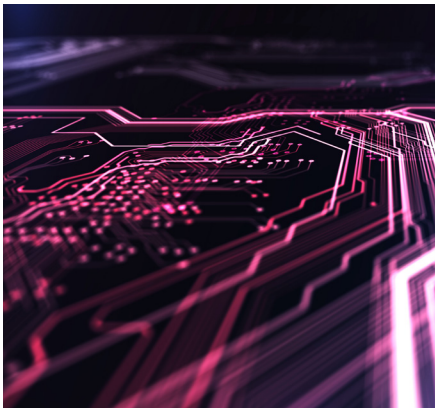


<< CYBERSCOUT CASE STUDY #1: *The Case of the Missing Laptop*

An employee at a small accounting firm took home her office laptop to do some work over the weekend. On the way there she stopped at the mall. Someone smashed her car window and stole the laptop, exposing the personal records of more than 120,000 people.

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. CyberScout's DataRiskStages® service, available to the firm through insurance, was able to assess the stolen computer's level of protection and advise the firm on how to notify each hospital and patient. With CyberScout handling the breach, the firm was able to stay in business.

Red River Mutual

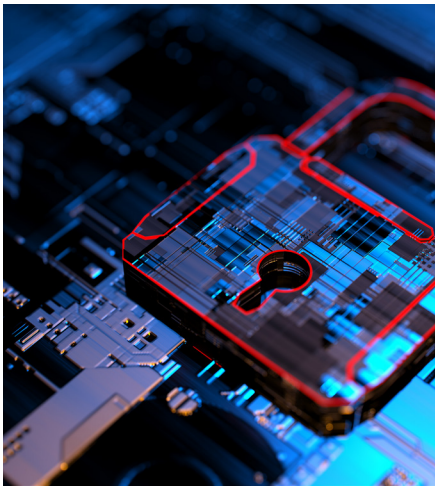


<< CYBERSCOUT CASE STUDY #2: *IT Oversight Leads to Breach*

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 concern about the personal data appearing on search engines. The sheriff's department contacted CyberScout to determine whether it should consider fraud remediation. CyberScout's 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.

CYBERSCOUT CASE STUDY #3: *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 bad guys gained access to nearly 30,000 credit card numbers dating back nearly five years. CyberScout suggested that the merchant filter out all the card numbers that were still active, which reduced the affected group to 12,000. Then CyberScout 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 the CyberScout Fraud Resolution Center where customers could get advice on further protecting themselves. CyberScout also helped the merchant prepare for litigation against the host who caused the breach in the first place.



<< CYBERSCOUT CASE STUDY #4: *Leased Photocopier Leads to Breach*

A news organization bought a photocopier that had once been leased to another 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 previsous leasee. The journalist contacted the company because it was planning a news segment about the data risks copiers pose to protecting sensitive personal information. CyberScout worked with the client to determine what information had been leaked and provided 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.

Your Story is Ours to Protect