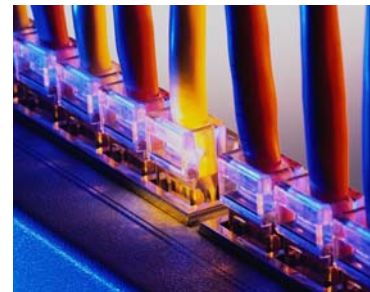




Privacy and Network Liability Insurance

If you haven't been hit by virus, spyware or data theft – LOOK OUT! YOU COULD BE NEXT! Although today's web-based technology and extensive networks provide companies with more speed and convenience than ever before, the benefits to all parties are fraught with new and complex risks. Vast amounts of sensitive, private information stored in accessible formats can fall into criminal hands by sophisticated hackers breaching network security, or by simple negligence. The resulting loss to the company includes not only the cost to repair corrupted data, but also costs to notify and compensate those affected.

Legislators have been scrambling to keep pace with the exponentially growing risks and many jurisdictions now have laws that outline the rights of individuals and potential sanctions for breach of such laws. The U.S. has led the way in implementing breach notification laws, mandating that organizations inform those individuals potentially affected by a security breach. Although Canada does not currently mandate notification, this may soon change. In the meantime, federal guidelines provide best practice recommendations.



Examples of recent publicly reported Canadian privacy/network security breach events include:

- **TJX/Winners:** Between 2002 and 2006 a hacker stole credit card and other personal information from 45.6 million customers of Winners/Home Sense. In Canada alone, thousands of cases of fraud were reported on stolen cards. The fallout included lawsuits by banks and shareholders (pension funds), class actions by customers, and regulatory probes in both the US and Canada
- **CIBC:** In January 2007, CIBC suffered the loss of a computer file in transit between offices with data on 470,000 customers
- **Passport Canada:** In December 2007, a security flaw allowed unauthorized access by the public to passport applicants' personal information on-line
- **Canada Post:** In December, 2007 Canada Post reported a security breach allowing the login records of scores of small businesses using its shipping website to become publicly available
- **Canadian Bar Association:** In January 2008, the CBA disclosed a security breach whereby unauthorized access was available to online orders and credit card information of its members
- **Bell Canada:** In February 2008, 3.3 million Bell customers had their personal information stolen. A suspect was arrested in Montreal, following which public disclosure of the breach was made.

Given the potentially devastating result of data and privacy breaches, boards, risk managers, finance departments and technology leaders are recognizing this new area of risk and their obligation to mitigate through increased security, contractual provisions with service providers and vendors, and through insurance. In the process, they are finding:

- Most organizations are exposed
- Most traditional policies do not cover these risks
- A privacy breach would have a major impact on brand and reputation
- No system can be designed to eliminate the potential for all loss, as people and process failures cannot be eliminated and insiders may be perpetrators
- Many functions are conducted by outside vendors and contractors who may lack insurance and assets to respond.



Executive Risk Insurance Services:

Recognizing the unique needs of the Canadian privacy environment, Executive Risk Insurance Services (ERIS) has developed a Canadian Privacy and Network Liability insurance policy. The policy is designed to respond to Canadian privacy and network security issues along with the exposures companies face worldwide.

Overview of Coverage

- **Privacy Liability**
 - Covers third party damages and claim expenses arising out of a Privacy Breach resulting in harm to employees or third parties
 - Covers amounts the assured is legally obligated to pay, including claims expenses, as a result of a penalty or sanction imposed by a federal, state or local regulatory body
- **Crisis Management and Notification Expenses**
 - Covers the expense incurred in attempting to mitigate reputational damage as a result of a Privacy Breach and the costs involved in notifying customers or employees
- **Security Liability**
 - Covers third party damages and claim expenses arising out of a failure of Network Security

Coverage Highlights

- Insurer has the duty to defend
- Insured has the right to elect counsel
- Insured may settle where Loss does not exceed 50% of the retention
- Insured may incur Notification and Crisis Management expenses prior to receiving consent by the Insurer and prior to a demand or proceeding
- No mandatory reporting of potential claims
- Insured only required to report Claims once a designated representative becomes aware
- Insured versus Insured exclusion does not apply to Privacy Liability
- Intentional violation of law exclusion not applicable where breach is required by law
- Breach of contract exclusion not applicable to Insured's own privacy statement or indemnification agreement
- Broad severability for exclusions, application and late reporting
- Worldwide Territory
- Broad definition of Claim to include:
 - Monetary and non-monetary damages
 - Formal administrative or regulatory investigation or proceeding commenced by a complaint made to the Privacy Commissioner
- Insured extended to include directors, officers, trustees, employees and independent contractors
- Vicarious liability for breaches of security by vendors for whom the assured is legally responsible
- Coverage for fines, penalties and punitive or exemplary damages to the extent permitted by law

For further information and a detailed **ERIS –Privacy and Network Liability Insurance** policy discussion, please contact your insurance broker or an **ERIS** representative: