

CYBER INSIGHTS

Digital Privacy Regulations are changing on November 1st - Will you be prepared?

Government regulations are changing on November 1st to amend the Personal Information Protection and Electronic Documents Act. This means that there will be a requirement in place to notify individuals of any breach in their personal information that could cause potential harm. There will also be added obligations to record all breaches of personal information and to report them to governmental authorities.

Review the details of your Cyber coverage as it may not fully respond to these liabilities. Contact your Jones DesLauriers expert Advisor today.

All Businesses and Organizations are at Risk

Any business or organization that collects personal information is at risk of a possible cyber breach, including both for-profit and non-profit businesses.

You are exposed to cyber risk if your organization collects, stores or distributes:

- Personal information for clients or employees
- Credit card information
- Health care data
- Banking records

Information breaches can occur at any level in your organization – from internal employee tampering to external malware and corruption of your IT systems. The risks are far-reaching, and the damages can be extensive.

Your Business is at High Risk for Cyber Breach

Any industry can be impacted by a cyber incident, and if your company has any of the following risk factors, your chance of an attack is even greater.

1. Outdated Anti-Virus Software especially on mobile devices where your organization doesn't control automatic updates.
2. Cloud Usage which can put your business at risk each time data is transmitted or stored.
3. Poor Password Practices as a high percentage of data breaches may be the result of weak passwords.
4. Lack of Employee Training on the ability to recognize phishing scams and differentiate legitimate requests from fake ones.

CYBER INSIGHTS

Unfortunately, many organizations are unaware of the possible liabilities and their need for appropriate insurance coverage. It's important to address these concerns before a problem arises, since compliance costs and legal implications could have a serious effect on the ability to provide service to clients going forward.

You can mitigate your chances of incurring a breach by:

- Creating a risk management plan
- Limiting access to sensitive information
- Increasing security protocols
- Conducting employee training on cyber safety
- Having a liability assessment to ensure you have the right amount of coverage

Can Your Budget Withstand the Cost of Remedying a Breach?

The cost of recovering after a breach of information can be steep. All potentially affected individuals must be notified, but beyond that, organizations must then incur damages for:

- Information gathering and distribution such as hotlines and correspondence
- Legal advice
- Mental health support
- IT services to assess and repair damage
- Public relations consultants to respond quickly to maintain your reputation

The average cost to recover losses and restore business is \$250 per record, which can climb very quickly to considerable amounts when faced with thousands of records at a time. A client base of 1,000 can translate into \$250,000 in fees, whereas a client base of 5,000 can amount to as much as \$1,250,000. Unfortunately, these figures do not include any potential law suits that may be filed for privacy infractions.

Failure to Report – a Costly Mistake

Non-compliance – either through failure to notify or failure to keep adequate records – can result in hefty fines imposed by the government. Amounts of up to \$100,000 per violation can be levied – even if the offense was committed in error.

CYBER INSIGHTS

It's Not a Questions of if, but When your Organization Will be Affected

Given the new regulations, many organizations have not considered their increased need for insurance coverage to mitigate costs of notification, reporting and record keeping, future regulatory fees and legal costs.

The best thing you can do to manage your cyber risk is to make sure you establish security and privacy procedures, and develop internet usage and social media policies for all staff. You should also check that you have adequate coverage to insure any losses you may incur. Jones DesLauriers has tools at our disposal to help you:

- Assess and manage risk
- Inform you of your obligations under the new Act
- Assist you in Implementing a breach response plan
- Ensure your coverage is sufficient in the event of a cyber incident – increased liability and notification expense limits may now be required

Given the amount of information we store electronically, it's not a question of if, but when your organization will be affected. Take steps now to sufficiently protect your organization from the costs of electronic breach of information.

Call your Jones DesLauriers Advisor today for a comprehensive risk assessment. If you currently have some form of Cyber coverage, it may not fully respond to these liabilities. Get sound advice to help you protect against data breach and prepare for the new November 1st Digital Privacy Legislation.

Jones DesLauriers Insurance Management Inc.
2375 Skymark Ave.
Mississauga, ON
L4W 4Y6
416.259.4625 877.232.9996
www.jdimi.com