CYBER INSIGHTS

LloydSadd INSURANCE BROKERS

NAVACORD®

www.lloydsadd.com

Cyber Breach Reporting Obligations and Response

Whether a breach of security safeguards affects one person or a 1,000, it will still need to be reported if your assessment indicates there is a real risk of significant harm resulting from the breach.

DO I NEED TO REPORT ALL BREACHES?

No. The law requires that you report any breach of security safeguards involving personal information under your control if it is reasonable to believe that the breach of security creates a real risk of significant harm to an individual. This includes personal information under your direct control and/or that may have been collected by a 3rd party on your behalf.

Factors that are relevant to determining whether a breach creates a real risk of significant harm include the sensitivity of the personal information involved in the breach of security safeguards and the probability the personal information has been/is/will be misused.

Click Here to find detailed information on how to assess if a breach of security safeguards poses a real risk of significant harm and needs to be reported.

Click Here to Report a Breach to the Federal Authorities

In addition, private sector organizations in Alberta must also report the breach to the provincial authorities. *Click here* to learn more.

WHAT TO DO IN THE EVENT OF A BREACH

1. Immediately contain the breach (e.g., notify IT, stop the unauthorized practice, recover the records, shut down the system that was breached, revoke or change computer access codes or correct weaknesses in physical or electronic security).
2. Document any and all actions taken from the time of the breach.
3. Escalate internally as appropriate, including informing the person within your organization responsible for privacy compliance.
4. Contact your Broker to report the breach to your Cyber insurer who will take immediate action to respond.
5. Notify legal counsel and determine the need to assemble a team to respond to the breach.
6. Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.
7. Activate any backups or recovery plans
8. Report to the authorities
9. Communicate impact of the breach to all affected parties
10. Take precautions to prevent future breaches

Ensure your business is properly protected against cyber attacks.

Contact Lloyd Sadd today to learn about your coverage options and how to prevent cyber attacks.

Source: Office of the Privacy Commissioner of Canada

LET US HELP YOU MANAGE YOUR RISK

Suite 700, 10240 – 124 Street,
Edmonton, Alberta T5N 3W6
1-800-665-5243

lloydsadd.com
navacord.com
info@lloydsadd.com