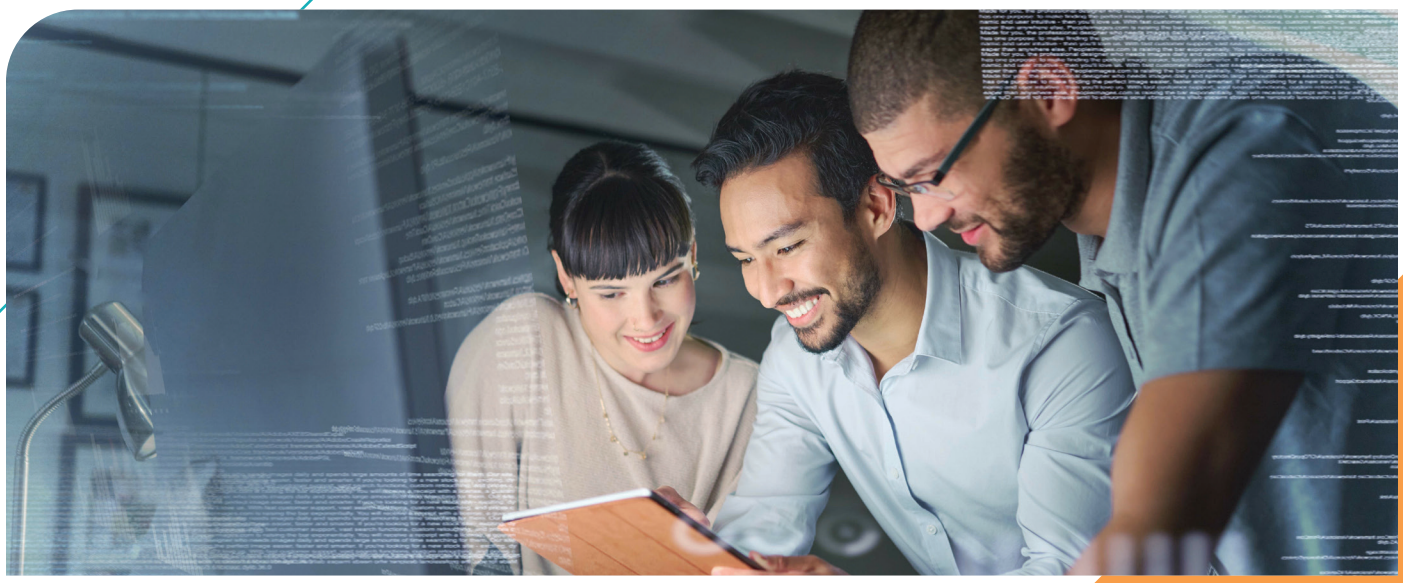
Preparing for and managing cybersecurity incidents



- Understand the legal and regulatory requirements that affect how your organization prepares for and responds to cyber threats.
- Establish an effective cyber risk management program to assess and prioritize threats and develop corresponding risk-mitigation strategies.
- Proactively prepare your organization's critical incident response plan with the help of breach counsel.

Confidently safeguard the data entrusted to you

Your organization faces risk from cybersecurity threats on a daily basis and must react quickly if an incident occurs. Both private and public sector organizations serve as stewards of valuable data, from health information to customer or member information to employee information. The potential damage and costs of a breach can be devastating for organizations of any size.

In the event of a data breach, you must take immediate action to safeguard the confidentiality, integrity and availability of your information assets and data. Proactively developing and continually refining a comprehensive cybersecurity and data protection strategy is key to preventing and reducing harm.

Skilled counsel with you every step of the way

Working closely with your internal team and external security experts, we help you manage cybersecurity risks, conduct strategic risk assessments and implement effective governance, risk transfer and incident response planning.

Our approach to cybersecurity, privacy and data breach preparedness is focused on minimizing, mitigating and managing risk.

MLT AIKINS

Effective cyber risk management requires proactive and ongoing legal support. We help your organization develop the framework that will help determine your current cybersecurity and data protection capabilities, set goals for a target state and establish the plan for improving and maintaining an effective cybersecurity/data protection program.

- **Know your obligations.** We help you understand the legal and regulatory requirements your organization must meet as it reacts to a cybersecurity incident – such as mandatory reporting and record-keeping or fulfilling contractual obligations.
- **Assemble your Cyber Incident Response Team (CIRT).** We can become part of your CIRT to proactively develop and implement a response plan. If an incident or data breach does occur, we can assume the role of breach counsel, giving your organization trusted legal guidance on immediate and longer term next steps.
- **Engage breach counsel.** Some of the breach counselling services we offer to clients include board training sessions, security assessment and tabletop exercise, insurance review, high-level privacy review, incident response plan review/preparation and vendor contract review. We offer three breach counsel packages, scaling our services to best meet your needs and desired investment.

1. Basic

Investment $5,000*

The Basic package includes the following:

- Board training session
- Connect with cybersecurity firm for security assessment and tabletop exercise**
- Attend tabletop exercise

2. Intermediate

Investment $10,000*

Everything included in Basic, plus:

- Insurance review
- High-level privacy review
- Incident response plan review/preparation

3. Advanced

Investment $20,000*

Everything included in Intermediate, plus:

- Vendor contract review
- Tabletop exercise

**Prices shown are legal fees and do not include disbursements or applicable taxes.*

***Assessment and tabletop exercise not included in price.*

Contact us

Kristél Kriel
kkriel@mltaikins.com
(306) 347-8614

Nathan Schissel
nschissel@mltaikins.com
(306) 347-8476

Contact our breach counsel team, any day, any time.

breachcounsel@mltaikins.com | (877) 257-0666

MLT AIKINS

WESTERN CANADA'S LAW FIRM