MARKEL

Cyber 360 Canada

Markel Cyber 360 Canada

We designed Cyber 360 Canada to safeguard businesses before, during, and after a cyber attack, to make sure you are protected and covered.

Through our panel of experts, we offer a range of support when you need it most. From breach response, incident management, legal, forensic investigation, credit monitoring, and call center management, loss control, and public relations, we're with you. And our 24/7 claims line means you can contact us any time a cyber attack happens.

First-party coverage summary:

– IT forensics costs

– Privacy breach notification and mitigation costs

– System and data rectification costs

– Business interruption costs

– System failure

– Critical service provider business interruption

– Critical service provider system failure

– Extortion costs

Extensions and enhancements:

– Betterment and bricking

– Crypto-jacking and telecommunications fraud

– Dependent non-IT service provider's business interruption & system failure

– Regulatory and voluntary shutdown

– Cyber theft and social engineering

– Reputational harm

Third-party coverage summary:

– Cyber and privacy liability

– Regulatory investigations and fines

– Payment Card Industry Data Security Standard (PCI DSS) investiations and fines

– E-media liability

Additional coverage options:

– Professional and technology services liability

– Directors and officers liability

– Employment practices and third-party discrimination liability

– Fiduciary liability

– Theft

MARKEL

Markel Cyber 360 Canada Incident Response

At Markel, our clients' safety and **security is our priority.**

Our transparent approach to breach handling is key to making our clients feel at ease. This means mapping out simple, clear procedures for what you should do – and what we do – if the worst happens.

From the moment your policy is bound, we're on your side. In a cyber emergency, the right preparation can be the difference between fixing a breach swiftly and a major incident unfurling.

In a breach scenario, our team of cyber breach coaches from leading global law firm, Norton Rose Fulbright, will act fast, following a streamlined approach in order to minimize disruption and get you back on your feet.

Norton Rose Fulbright Cybersecurity Services:

Led by 2025 Chambers-ranked lawyers Imran Ahmad and John Cassel, Norton Rose Fulbright brings exceptional expertise in bilingual cybersecurity and data privacy, supported by Canada's largest dedicated team. As trusted advisors to Fortune 100 companies, they play a critical role in helping organizations proactively prepare for and effectively respond to cyber threats.

Norton Rose Fulbright has been advising clients on managing breaches, and cyber incidents for thousands of clients around the world. The team combines sector expertise with international reach as data breaches know no borders. They can readily draw on partners specializing in privacy and breach response across Canada and the United States, as well as in over 50 cities spanning five continents.

- **24/7, 365 bilingual support**
- **+1000 cyber incidents handled to date**
- **Cyber security partner network across Canada, North America, Europe, Africa, Asia and Australasia.**

MARKEL

CYBER INCIDENT RESPONSE WORKFLOW

At Markel, our cyber clients' safety is our priority.

The key to making our clients feel at ease is our transparent approach to a breach. This means mapping out simple, clear procedures for what you should do – and what we do – if the worst happens.

Markel Cyber 360 Canada - Breach Timeline

01 — 1 HOUR — Suspected breach – initial action

Our cyber breach coaches act as notification agents and are available 24/7, 365. Notifications can be made directly via their hotline or email. Contact details are also included in policies, allowing insureds to notify them directly.

Jurisdiction

Where the insured or breach event appears to be in Quebec, they will defer to the most appropriate language.

Conflict checks

Our breach coaches typically receive a response in less than 1 hour during business hours. Our breach coaches never delay taking the first call with the insured. If the results of the check have not arrived, they will explain this to the insured.

Breach triage

Triage call to identify incident and scope of services required. If no services are required, our breach coaches will not charge for the time incurred.

Where further assistance is anticipated, breach coaches will:

- Explain product, services and potential costs
- Establish services required, including whether Canadian or overseas assistance is required, and determine appropriate subcontractor(s) to assist
- Immediate incident risk management crisis advice, including first legal advice on risks of data breach
- Summary of incident notification and seek Insured's consent to share with Insurer

Where further assistance is required, breach coaches will:

- Issue retainer letter to insured, including subcontractor services provision
- Issue report to Insured outlining discussion, options and next steps
- Convene further call with cyber panel vendors within 2 hours

02 — 24 HOURS — Analysis, reporting and breach management

- Breach coach provides services on behalf of insured.
- All cyber vendors coordinated by our beach coaches will explain the extent of their services being provided to the insured.
- Work with IT consultants to contain, remediate and investigate incident.
- Provide legal advice on regulatory and legal issues arising out of the incident, including whether notifications required to the appropriate regulatory authority.
- Provide insured with 24-hour incident report.
- Consider whether immediate notifications required (e.g. if Data Processor to Data Controller or if required under industry-specific regulations).
- Continuous assessment of whether involvement of other subcontractors (e.g. Ransomware negotiators) are required.

MARKEL

03

24-72 HOURS

Mitigation and investigation

- Blended incident risk management and legal services.
- Advisory on any data breach issues and potential notifications to regulators or data subjects.
- Advisory on other legal issues including protective steps in respect of litigation and reputation management.
- Directed by our breach coaches, IT consultants containment typically complete. Remediation and investigation ongoing.
- Directed by our breach coaches, other cyber panel vendor provide services such preparing press releases, formulating notification communications and activating notification agents/credit monitoring providers.

04

72 HOURS+

Conclusion

- Breach coaches continue to provide blended IRM and legal services at insureds' discretion.
- Breach coaches provide legal advice including responding to regulatory investigations, defending claims by counterparties and affected data subjects, and advising on recovery options.
- IT consultants complete remediation and investigation and close out tasks.
- Any other sub-contractors conclude activity.
- Final report.
- Any potential business interruption costs are formulated and prepared.

Get in touch with our expert Markel Cyber underwriting team.

We target a wide spectrum of industries and have the flexibility to consider the unusual. Markel offers a variety of risk management resources and services to our Cyber 360 customers.

Our Team

Ed Rawe
Assistant Vice President, Cyber
437-215-6881
Ed.Rawe@markel.com

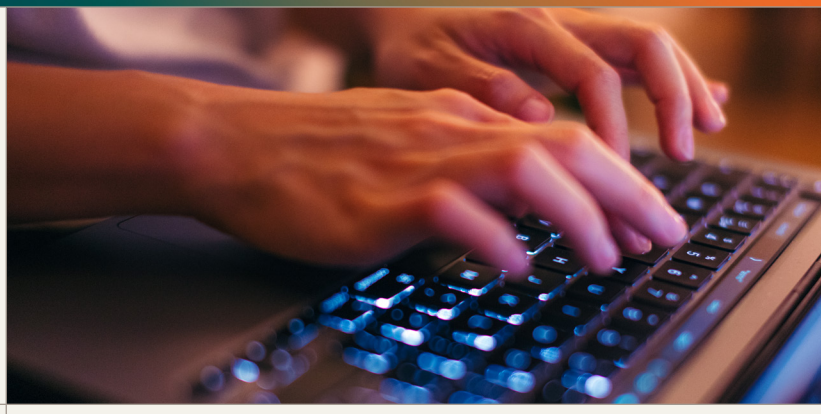
MARKEL

Markel Cyber 360 Canada Vendors

Markel partners with a variety of non-exclusive experts to ensure you have the resources you need before, during, and after a cyber incident. This list of core vendor partners is not comprehensive; additional providers may be engaged as needed.

If you are experiencing a security incident, our support hotline will connect you to services and resources to rapidly address an insured event 24/7, 365.

Contact: Norton Rose Fullbright L.L.P.
1-866 -BREACHX / 1-866-273-2249
nrfc.breach@nortonrosefulbright.com



Breach coach services

Legal counsel specializing in cyber and privacy events. Counsel assists in interpreting state regulations, responsibilities under the law, drafting customer notice letters, and coordinating with subject matter experts.

Norton Rose Fulbright LLP

Data restoration firms

Firms specializing in cybersecurity breach recovery, with services that help organizations swiftly restore operations and data after a cyberattack.

Arctic Wolf

Fenix24

Forensics and restoration

Third-party experts who assist in investigation and remediation.

Mandiant

Kroll

Crowdstrike

Arctic Wolf

Ransom negotiations

Third-party expert negotiators, with deep insight into threat actors and a track record of securing favourable outcomes.

One Arrow

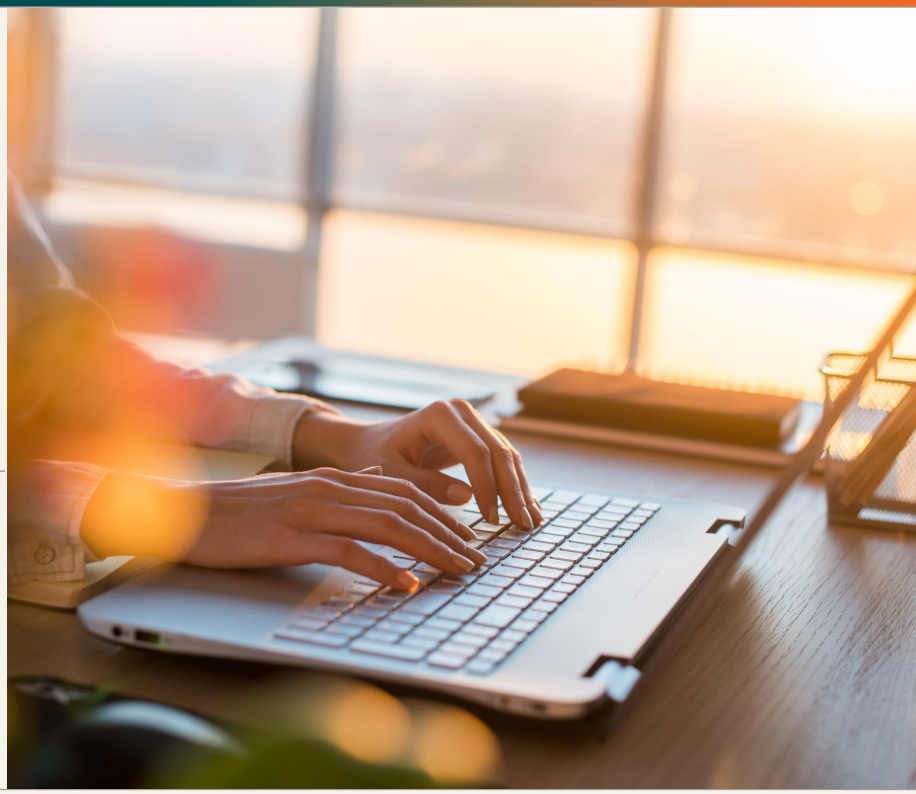
Cyber Steward

Markel Cyber 360 Canada
Guardian 360 Pre-Breach Services

All Cyber 360 clients can benefit from a claims on-boarding call to find out more about how the Markel Cyber Claims and our Breach Response partners can assist in the event of a cyber incident. As part of this support, clients will also have access to the Black Kite platform — a leading provider of third-party cyber risk intelligence — which offers a non-invasive IP scanning assessment to help organizations better understand and manage their cyber security risk.

Markel Cyber 360 Canada is built to support your business through every phase of a cyber incident— before, during, and after— keeping you one step ahead.

In response to growing demand for proactive protection, eligible policyholders may also receive access to one of the below Guardian 360 offerings, alongside their pre-breach onboarding call and Black Kite access. Each Guardian 360 product includes a curated menu of cyber and privacy services, and policyholders can select one preferred service to activate under their coverage.



Guardian 360 Core

Breach partners may provide updates on Privacy, Cyber and AI, or an initial cyber risk consultation or contract review service, as detailed below:

1. Weekly privacy update newsletters, along with exclusive access to quarterly roundtables focused on Privacy, Cyber & AI —bringing together industry peers and experts for timely insights
2. High-level review of your current cyber security governance policies and procedures and strategic discussions of legal and regulatory obligations, and identification of immediate high-risk areas
3. Review of up to two critical contracts with insights on potential risks

Guardian 360 Plus

Breach partners may provide cyber risk assessments, tabletop exercises or contract reviews, including:

1. Conducting a cyber risk assessment review of an existing incident response plan, or support in developing one, and identifying gaps in compliance with major regulations
2. A virtual one-hour tabletop exercise with key stakeholders
3. Customized checklist mapping relevant federal and provincial cyber regulations
4. Review of up to five critical contracts with insights on potential risks

Markel Cyber 360 Canada Services

Guardian 360 Pro

Breach partners may provide a comprehensive policy review, custom tabletop exercise, regulatory compliance checklist or contract review, as detailed below:

1. Comprehensive review of up to two key policies—such as incident response or data retention—with expert recommendations to align with legal requirements and industry best practices
2. A tailored two-hour virtual tabletop exercise based on specific industry and risk profile, followed by a debrief and feedback session to reinforce preparedness
3. Customized checklist outlining applicable federal and provincial cyber regulations
4. Review of up to five critical contracts, offering insight into potential risks and recommended clause enhancements to support compliance and resilience

Guardian 360 Ultra

Breach partners may provide a full cyber readiness assessment, incident response plan drafting, custom tabletop exercises, regulatory gap analyses, board/executive training or vendor management consultancy, as detailed below:

1. Full review of all cyber policies, procedures, and contracts, along with interviews with key personnel to assess preparedness
2. A three hour immersive tabletop exercise featuring real-world scenarios, live feedback, and strategic decision-making with a detailed summary of lessons learned, key takeaways, and a prioritized action plan for improvement
3. A regulatory compliance review: expert gap analysis of your alignment with applicable cyber laws and regulations
4. Cyber risk training for leadership teams: customized training for executives or board members, including legal obligations and real-world case studies
5. Vendor management expert advice including a risk assessment template and standard recommended cyber clauses for contracts and vendor agreements for ongoing resilience