Cyber Resilience Toolkit: Breach Response Plan Guide

Why Every Company Needs a Breach Response Plan

Claims are inherently disruptive, and despite the amount of insurance you carry, recovering from a cyber incident is difficult without a well-prepared plan.

Cyber events such as ransomware, data theft, or fraudulent payments can halt operations, erode trust, and threaten financial stability. From an insurance perspective, your ability to recover costs under a cyber policy depends on the actions taken immediately after a breach or suspected breach. From a business continuity perspective, the strength of your breach response plan determines how effectively you can contain the incident, restore operations, and protect your reputation.

This guide is designed to help companies build an internal breach response and notification plan that both maximizes recovery under the cyber insurance policy and reduces operational and reputational disruption.

Breach Response Plan Objectives:

1. Preserve insurance coverage by notifying the insurer within the required timeframe.
2. Access insurer-approved resources without unnecessary costs.
3. Meet contractual obligations owed to clients, vendors, and partners.
4. Comply with regulatory requirements for reporting and data protection.
5. Demonstrate maturity in risk governance, strengthening your position with insurers, investors, and regulators.

Key Elements of a Strong Breach Response Plan

1. Clear Trigger Events

- The plan should specify which events activate the response process, such as:
- Unauthorized access or data exfiltration.
- Malware, ransomware, or other system compromises.
- Third-party vendor breaches affecting your systems.
- Fraudulent payments or cybercrime attempts.
- Any suspicious activity likely to trigger insurer response costs.

2. Immediate Containment and Escalation

The first 1–4 hours are critical. Your plan must define how IT and security teams:

- Isolate affected systems and preserve evidence.
- Escalate to legal, executive, and insurance coordinators.
- Document facts, timelines, and impacted assets.

3. **Insurance Notification**

Cyber policies require notification as soon as practicable:

- Notify the insurer's breach response team and your broker.
- Provide initial facts, containment steps, and a point of contact.
- Avoid hiring external vendors without prior approval from the insurer to preserve coverage.

4. **Coordination with Approved Vendors**

Policy requirements around vendor usage vary by insurer, making it essential to consult your broker to understand your insurer's position. Some insurers require you to use their pre-approved experts, while others permit you to select your own vendors and seek reimbursement, though coverage may be reduced if non-approved vendors are engaged.

Working with your broker to identify a panel of trusted vendors can greatly enhance the speed and effectiveness of your breach response plan. Key vendor categories include:

- Incident response
- Forensic investigation and remediation
- Legal and regulatory counsel
- Notification and call center services
- Crisis communications and public relations
- Post-breach remediation

5. **External Notifications**

Your obligations extend beyond your insurer. The plan should map responsibilities for notifying:

- **Regulators:** Privacy Commissioner for personal data breaches, as applicable
- **Individuals:** Affected persons where there is a risk of harm
- **Law Enforcement:** If criminal activity is suspected
- **Clients, Vendors, Partners:** Where contracts require disclosure or actual or suspected breach.

A comprehensive analysis of your disclosure obligations should be conducted periodically, particularly with respect to client, vendor, and partner contracts.

6. **Documentation and Reporting**

Insurers and regulators expect complete records, and we recommend maintaining a single folder containing the following documents for ease of access:

- Discovery and response timelines.
- Communications with insurer and vendors.
- Diagnostic and forensic reports that support the cause of the incident
- Breach ledger (maintain for 24 months)
- All breach-related costs incurred.

7. **Post Incident Review**

Within 30 days of resolution, conduct a lessons-learned review and update policies, controls, and training. This not only strengthens your security posture but also demonstrates to insurers that your company actively manages and mitigates cyber risk.

The Role of Contractual Obligations

In addition to regulatory duties, many companies are bound by contractual obligations to clients, vendors, and investors. These may require:

- Immediate disclosure of any data breach, whether actual or suspected
- Specific timelines for notification.
- Liability for costs incurred by counterparties.
- Demonstrations of corrective action post-incident.

A breach response plan ensures you do not inadvertently breach these agreements, which could otherwise trigger litigation, indemnification demands, or reputational damage.

Broker's Perspective

As your insurance broker, our role is to help you:

1. Align your breach response plan with insurance requirements so coverage is preserved.
2. Identify contractual reporting obligations and ensure they are built into your plan.
3. Coordinate with insurers during a live incident.
4. Position your company as best-in-class when negotiating renewals or new coverage.

Companies that can demonstrate a clear, tested breach response plan respond more effectively to incidents, secure stronger insurance terms, and build greater confidence with stakeholders.

Next Steps

We recommend:

1. Reviewing your existing breach response process against these elements.
2. Contact our office for a breach response template.
3. Mapping all regulatory and contractual reporting obligations relevant to your operations.
4. Conducting a tabletop exercise to test readiness.
5. Engaging us to support policy alignment and insurer coordination.

Reach out today for help designing a breach response plan.
We'll provide insights and schedule an advisor review to help secure your business.

Contact Us

Chris Jones
Account Executive,
Mining & Technology
+1 (778) 788-2853
Chris.Jones@axisinsurance.ca

Clive Bird
Senior Vice President,
Mining & Technology
+1 (604) 817-8072
Clive.Bird@axisinsurance.ca

Stacey Copeland
Vice President,
Mining & Technology
+1 (604) 619-7775
Stacey.Copeland@axisinsurance.ca

Tristan Smith
Business Development Specialist,
Mining & Technology
+1 (416) 885-0671
Tristan.Smith@axisinsurance.ca

About

Axis Insurance – Safeguarding the Exceptional. Axis Insurance is your strategic advantage; we cut through the complexity of risk management enabling you to confidently embrace the opportunities of tomorrow. Our role is to provide you with the best insurance value that combines coverage, service and price. We also provide personalized, quality service that includes professional insurance advice, ongoing policy maintenance and claims support. When any issue arises regarding your insurance coverage, we are your advocate, using our professional experience to best represent your individual interest. Follow Axis on LinkedIn, X, Facebook and Instagram. Stay up to date by signing up for our newsletter here.

axisinsurance.ca
#2000 – 1055 Dunsmuir Street, Box 49264, Vancouver, B.C. V7X 1L2
1-800-690-7475