CYBER LIABILITY CLAIMS PROCESS

When it comes to notifying your insurance company of an actual (or potential) cyber liability breach, the most important thing to remember is to report the incident as soon as possible. The insurance company's cyber team is there to help you through the process and handle the forensic investigation. Never try to investigate a cyber liability breach on your own, as it can hinder the investigation itself and potentially lead to more harm.

When calling the insurance company to report the incident, it is important to have the following information:

1. Policy number
2. Effective and expiration date of the policy
3. Point of contact for the claim (including a direct phone number and e-mail address – do not provide a general email address or phone number as this can delay the investigation)
4. Date of claim/cyber breach (always let them know if it is a potential or actual incident)
5. Description of the cyber breach (including city, state and event that led you to discover the incident)
6. The type of personal and/or confidential information that the breach impacted
7. Number of individuals and electronic devices that were compromised due to the breach

Please also be prepared to send the insurance company all relevant information related to the case such as reports, screenshots, documents, etc., as it better prepares them for the investigation. Again, it is important to first report the incident itself, even if you do not have all of the needed information.

We support our customers before, during, and after security incidents

Cyber incidents come in many forms — from ransomware, denial of service attacks, data breaches, social engineering, wire fraud, and technology failures. While each event is different, there are certain elements you can expect and Coalition is your partner in solving cyber risk before, during, and after an incident occurs.

Incident Timeline

First notice of event
Policyholder suspects a security concern and/or receives an alert from Coalition, and contacts Coalition using one of the three methods to reach Coalition.

Assessment and triage
Working with you, Coalition's team determines if there is sufficient reason to complete a forensic investigation. Indicators we look for: Legitimate logins to email, password changes, new accounts created, malicious email headers. Coalition's team will also work to triage any immediate security needs.

Engage
Coalition will coordinate the use of counsel and vendors so stakeholders will remain connected and informed.

Forensics
At the direction of counsel, Coalition Incident Response (CIR) or a 3rd party vendor completes forensics work and remediation where needed.

Recovery
Coalition ensures the payment of claim expenses and enables the policyholder to get back to business.

Our panel

To supplement our in-house abilities, we have an extensive network of panel providers to help you work with highly specialized firms during any cyber event. We even offer 2 hours of free legal counsel. Our panel providers are available here.

How to report an incident or claim

There are several ways to report a claim or suspected incident. With either method, you will connect with a member of our claims team.

- **Call:**   1 (833) 866-1337

- **Email:**   claims@coalitioninc.com
              claims@coalitioninc.ca (Canada)

- Contact us via **live chat** from our site to talk to a member of our team in minutes

Have a security question?

For general security questions, you can also email help@coalitioninc.com, (help@coalitioninc.ca in Canada), or you can reach out to the Coalition Incident Response team (CIR) at cir@coalitioninc.com. We can help you by answering security questions and identifying potential incidents that could be reported as a claim.

45%

Percentage of incidents that Coalition's Security and Incident Response Team fully contains ($0 cost to the policyholder and zero erosion of the policy limit)