

This guide aims to provide an overview of the cyber insurance claims process. Arch's Cyber Claims team works with you to make the claims process fast and flexible. Understanding the process empowers you to navigate a claim confidently in collaboration with our team of experts. Adjustment of each claim will vary depending on the facts and complexity of the claim and any specific issues that may arise.

### Arch Cyber Claims Contacts

**Deanna Cain** VP Claims  
M: 647 242 3904 | [dcain@archinsurance.com](mailto:dcain@archinsurance.com)

**Katherine Solomon** Technical Claims Manager  
D: 416 309 8223 | [ksolomon@archinsurance.com](mailto:ksolomon@archinsurance.com)

## Phase 1: Identify and Recognize the Occurrence of a Cyber Incident

How do you know if a cyber incident has occurred?

- Was there actual or suspected unauthorized use of or access to any computer system, including email?
- Have you lost, or was there unauthorized use of or access to, employee or customer private information?
- Was there damage to, or were you unable to access, any computer system due to a malicious use, attack or exploit of the computer system?
- Has a formal complaint or lawsuit been made against your organization relating to a network security breach or privacy violation?
- Have you, or do you suspect you may have, wired or transferred funds to a fraudster?

If the answer to any of these questions is "yes," or you suspect the answer may be "yes," contact **Arch Canada Cyber Claims**.

### Arch Insurance Canada Ltd. Cyber Claims

During business hours (8:30 a.m. – 4:00 p.m. ET, Monday-Friday)  
Toll-Free Phone (from U.S. and Canada only)  
D: 866 993 9978 | F: 416 309 8144 | [archcanadaclaims@archinsurance.com](mailto:archcanadaclaims@archinsurance.com)

### After Hours Claim Reporting

After hours or statutory holidays  
M: 888 852 3596  
[cyber.canada@dwfgroup.com](mailto:cyber.canada@dwfgroup.com) | [cyber.canada@dwfgroup.com](mailto:cyber.canada@dwfgroup.com)

When reporting a claim, please ensure you have the following information available when reporting a new claim:

- Arch Insurance policy number.
- Date of loss and/or incident and details of the incident.
- Your insurance information.

## Phase 2: The Claims Process

**1**

### Notice.

The claims process begins when the policyholder reports a claim or incident to Arch Canada at [archcanadaclaims@archinsurance.com](mailto:archcanadaclaims@archinsurance.com).

**2**

### Arch Response.

Arch receives the claim, assigns an Arch cyber examiner to triage the incident, review the claim, gather information about the incident, and review coverage.

**3**

### Policyholder Response.

Select or approve a Network Security Breach Counsel (NSBC) and Data Forensic Incident Response (DFIR) from the approved panel list. If the policyholder wishes to select a NSBC or DFIR that is not on the approved panel list, the policyholder must contact their Arch cyber examiner to obtain consent prior to any engagement.

**4**

### Communication.

The policyholder, Arch cyber examiner, NSBC, broker and DFIR provider attend a scoping call to discuss the circumstances of the incident. The experts advise on how to manage the incident and gather information to provide a DFIR statement of work that outlines the work anticipated to respond to the incident.

**5**

### Investigation.

DFIR investigates the incident to determine the root cause of the breach. In the event there is a cyber extortion, DFIR initiates the process to engage the threat actor making the ransom demand. NSBC analyzes the findings of the incident to determine the legal obligations.

**6**

### Conclusion.

The root cause is identified where possible and recovery steps are taken. If possible, DFIR decrypts the system and restores the data and network. If required, NSBC notifies the impacted individuals of any data breach. The Arch cyber examiner will assign liability defence counsel if necessary.

**7**

### Post-Recovery.

- The Arch cyber examiner facilitates payments to NSBC for legal services, to DFIR for investigation and restoration services, and to any other vendors whose services were deemed reasonable and necessary and approved by the Arch cyber examiner. Payments will only be issued by the Arch cyber examiner for amounts incurred in responding to the Claim that is in excess of the policy's self-insured retention.
- If the claim caused a business interruption or extra expense to be incurred, the policyholder submits a notarized proof of loss outlining these costs with supporting documentation. To the extent coverage is available for business interruption and extra expense loss, the Arch cyber examiner facilitates payment for such loss.
- The file is closed.

## Arch Canada Preferred Cyber Vendors

Digital Forensics and Incident Response	Services in French
Arete	No
Charles River & Associates	Yes
Coalition Incident Response	No
Crowdstrike	Yes
CyberClan	Yes
Stroz Friedberg	No
Law Firms	Services in French
Borden Ladner Gervais LLP	Yes
DWF Claims Services	Yes
Norton Rose Fulbright	Yes

Credit Monitoring	Services in French
Equifax	Yes
TransUnion	Yes
Notification	Services in French
Epiq	Yes
Kroll	Yes
Other Pre-Approved Vendors	Services in French
Forensic Accounting Williams C. Lewis Forensic Accountants Inc.	Yes
Public Relations/Crisis Management National Public Relations	Yes
Restoration and Recovery Services Fenix24	Yes

The listed above have been pre-approved by Arch. Coverage for the services provided by these firms is subject to the terms and conditions of your insurance policy.