GLOBAL CYBER & TECHNOLOGY PRACTICE

Cyber Insurance Claim Best Practices Guide

Guidance for navigating the cyber insurance claims process

July 2022

LOCKTON®

Cyber events are becoming more common and disruptive to organizations.

Those with the foresight to carry cyber insurance will be better prepared to promptly respond to a cyber event and insulated from the most severe financial consequences. They will be able to deal with crises efficiently and effectively, as they will have access to their insurers' specialized suite of incident response services at discounted hourly and/or project rates.

The cyber claims process is not always intuitive and easy to understand. Steps that might seem like common sense can sometimes create insurance difficulties. And cyber claims are very different from other types of claims because of the unique nature of the risk and the policies.

For that reason, it is critical that organizations know how and when to engage insurers. Insurance recovery depends on proper claims management. This guide is intended to provide the necessary framework to ensure your cyber insurance claim process is successful.

What is a cyber claim?

Cyber policies are unique because they provide both first-party and third-party cover. First-party cyber claims are distinct because they are often triggered by the discovery of a suspected or actual security event, requiring a sense of urgency and immediate access to technical services.

FIRST-PARTY COVERAGES

Compensate insureds for their own losses resulting from covered cyber events. Claims may arise from breaches, suspected breaches, suspicious activity on networks and cyberattacks.

EXAMPLES INCLUDE:

- A stolen laptop with confidential information.
- A hacked computer system.
- Business email compromise caused by phishing.
- A ransomware attack.
- A denial-of-service attack.

THIRD-PARTY COVERAGES

Pay others for insureds' liability to them for losses arising from covered cyber events and/or wrongful acts. Claims can include written demands, tolling agreements, arbitration demands, regulatory inquiries and complaints.

EXAMPLES INCLUDE:

- A demand for arbitration related to the disclosure of confidential information.
- A class-action complaint for violations of laws that protect consumers' personally identifiable information.
- A regulatory inquiry regarding the organization's handling of confidential data.

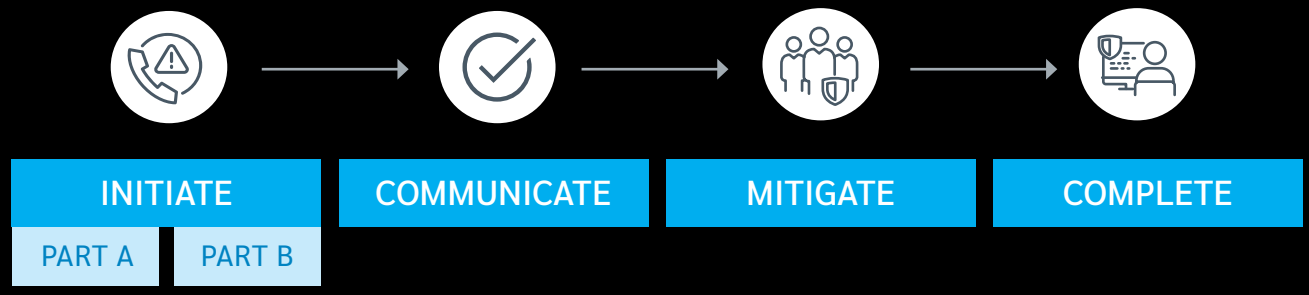
Cyber policies typically cover the reasonable and necessary expenses to investigate and remediate a covered incident as well as resulting business interruption losses. Such expenses can include legal advisors — which, depending on the jurisdiction, may be referred to by insurers and in policy language as "breach and/or privacy counsel" or similar language — forensics and public relations.

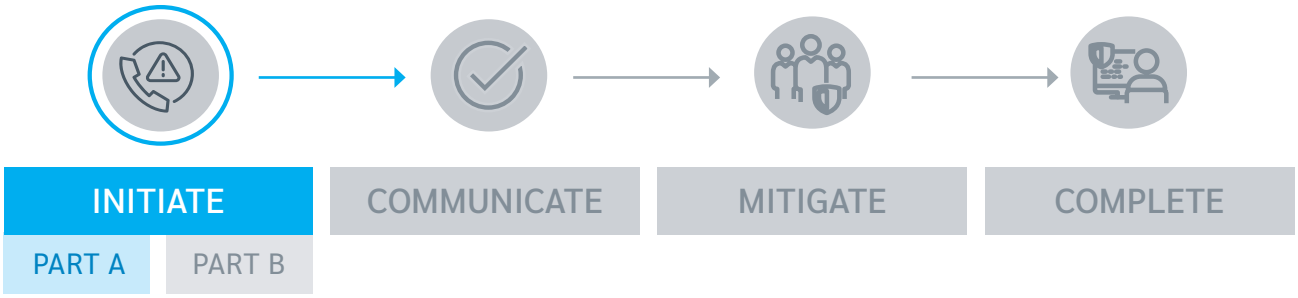
It is extremely important to remember that some matters may implicate more than just a cyber policy. For example, a phishing email resulting in a loss of funds may implicate both a cyber and crime policy. A lawsuit alleging violations of employees' privacy rights may implicate both a cyber and employment practices liability policy. And a ransomware attack may trigger a kidnap and ransom policy.

How does the cyber insurance claim process work?

Each cyber insurance claim is unique and will have its own nuances. Several factors — both internal and external — will determine how a claim proceeds and how long the process will take. These factors can include the type of incident and its scale, the threat actor's identity, and the organization itself — its industry, its information and operational technology infrastructure, and the robustness of its incident response and business continuity plans.

We have outlined over the next few pages the steps and best practices for organizations to consider when faced with a cyber insurance claim. The claim process will often run in parallel with an organization's incident response process.





As soon as possible, initiate the claims process by reporting to your insurer(s) directly through the dedicated hotline number AND contact Lockton to assist with reporting.

- NOTIFY INSURERS AS SOON AS PRACTICABLE to preserve rights under the policy(ies). This is often a condition precedent to coverage under the policy — in other words, the insurer must know about the incident and/or claim promptly so that it can respond and provide policy benefits if the matter is covered.
  - Claim expenses can increase when the insurer is not timely engaged. Organizations should ensure receipt of a written record that the insurer has acknowledged receiving the claim.
  - Insurers routinely refuse to pay for expenses incurred before the insured provides notice. If the insured provides notice after the policy or any prescribed post policy expiration reporting period expires, the insurer will almost certainly decline coverage for the entire claim.
  - Organizations sometimes think that a matter may be limited in size and scope, that it can be resolved within the policy retention, and that they do not need to notify their cyber insurers. That is not the case under most cyber policies, which typically require notice of every cyber event as soon as it is practical to do so.
  - Insurers have significant experience with cyber claims and are often able to provide advice on how other organizations have dealt with the same or similar events or threat actors.
- ERR ON THE SIDE OF TIMELY REPORTING rather than waiting and potentially being barred from coverage completely. Along with reporting the claim in a timely manner, organizations should ensure they have received written correspondence from their insurers acknowledging receipt of their claims.

Notification to insurers and/or Lockton should be built into incident response plans. Amid a crisis, this critical step to insurance recovery should be accounted for and executed upon.

Ensure that there is one person within the organization who is responsible for answering inquiries from and communicating with the insurer. That person may not have all of the answers, but should have access to those individuals who will have the information requested by the insurer about the claim. Ideally, the designated individual and a backup would be included in the organization's incident response plan.

INITIATE | COMMUNICATE | MITIGATE | COMPLETE

PART A | PART B

An organization's cyber insurance policy type will generally determine the organization's level of involvement in the selection of legal advisors and other vendors to help respond to the incident.

THERE ARE TYPICALLY FOUR TYPES OF VENDOR SELECTION PROVISIONS IN POLICIES:

Insurer selection

The insurer makes all decisions about the selection and retention of legal advisors and vendors.

Mutually agreeable

The insurer and the insured can mutually agree on the selection and retention of legal advisors and vendors. In the event of a conflict between the insurer and insured's chosen legal advisor and vendors, the insurer's decision will be final.

Insured selection

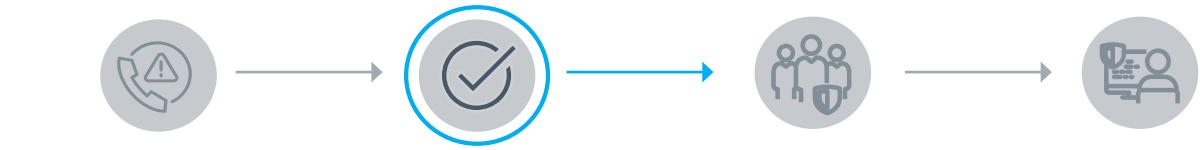
The insured has the right to select and retain legal advisors and vendors, but must receive the insurer's consent before any engagement.

Policy Endorsement

Prior to policy inception, the insured's chosen legal advisor and vendors and their hourly rates have been endorsed onto the cyber policy. The insured is permitted to proceed with the legal advisor and/or vendors as endorsed onto the policy.

If an insured organization is involved in the legal advisor selection process, it should:

- Review the insurer's panel of legal advisors.
- Consider local, state, and international obligations when selecting legal advisors.



INITIATE | COMMUNICATE | MITIGATE | COMPLETE

PART A | PART B

As your organization commences its investigation into the incident to determine the size and scope, keep in mind these cyber claims best practices:

- COLLABORATE with insurers and OBTAIN CONSENT on a proposed course of action, retention of vendors, hourly rates for vendors and settlement offers.
  - A common — and expensive — mistake for many organizations is retaining legal advisors and vendors without checking with insurers. Many policies give insurers the right to appoint vendors, while others allow insureds to select vendors from an insurer's panel. Even if a vendor is believed to be on an insurer's panel, communication with and written consent from insurers is crucial.
  - An insurer may not consent to retaining a vendor that is not on its panel; in this situation, an insurer will not reimburse the insured for any amounts paid to the vendor and will not recognize that any such payments reduce the policy retention. Even if an insurer consents to a vendor not on its panel, it may only agree to pay a rate that is consistent with what it pays its panel vendors — with insureds obligated to pay any difference.
- COORDINATE with legal advisors to select additional vendors as appropriate, including forensic specialists, public relations advisors, ransom negotiators, IT consultants and crisis management firms. If a legal advisor leads the vendor retention process on behalf of an insured organization, the vendors' work may be protected by certain privileges and doctrines, such as attorney-client privilege in the U.S.
- COOPERATE with insurers' efforts to evaluate potential claims and available coverage as it is a condition of policies. This can be accomplished by communicating early and often with insurers about the status and progress of a matter and any actions taken in response.

INITIATE | COMMUNICATE | **MITIGATE** | COMPLETE

PART A | PART B

Work with legal advisors and the designated incident response team to mitigate the incident — including (as required) notifying affected individuals, law enforcement and regulators; providing credit monitoring; and implementing appropriate crisis communications.

Follow these steps to mitigate any potential negative claims consequences:

- ENSURE all scopes of work are sent to and approved by the insurer.
- SCHEDULE periodic check-in calls with insurer to confirm the insurer has all necessary information.
- MAINTAIN detailed records and documentation regarding any business interruption losses.
- ENGAGE Lockton to ensure the claim proceeds in an orderly fashion.

INITIATE | COMMUNICATE | MITIGATE | COMPLETE

PART A | PART B

As you remediate and complete your organization's investigation into the incident, consider taking the following steps:

- DEBRIEF and REVIEW lessons learned from the incident and accompanying response.
- Engage a FORENSIC ACCOUNTING firm to assist with business interruption losses.
  - When a cyber event results in a business interruption, certain resulting losses are covered under many cyber policies. Few organizations understand how to present such a claim to insurers in a way that will get it paid quickly. Experienced forensic accounts can provide valuable assistance to insureds, helping them prepare proofs of loss, provide insurers with the information they require, and respond to questions from forensic accountants retained by insurers to evaluate claims.
  - Some costs associated with retaining a forensic accountant to assist with quantifying business interruption losses may be covered by a cyber policy — it is important to check with the insurer and obtain confirmation that those costs are covered.
- If the incident results in third-party litigation, review the insurer's panel to consider selection of litigation legal advisors, if selecting legal advisors different from those who were part of the incident response and provide notification to insurers about any third-party claims received.

Frequently asked questions

How long will the claim process take?

This will depend on the complexity of the claim and any potential coverage issues that arise. A simple data breach can take nine to 12 months from notification to claim resolution, but the timeline can change if facts discovered during the investigation require additional review and mitigation measures. A sophisticated ransomware attack, with resulting business interruption losses, can take nine months to two years from notification to insurers to claim resolution. A class action for compromises of personally identifiable information will depend entirely on the particular jurisdiction and the court docket of that jurisdiction. And a regulatory inquiry will proceed based on a regulator's timetable.

Why should our organization use panel vendors?

Insurers scrutinize privacy firms' qualifications and capabilities before allowing them to be on their panels. Insurers also negotiate hourly rates with panel vendors that are significantly lower than the cost to privately retain those vendors.

Moreover, a panel firm knows the insurer's reporting requirements and billing guidelines, so they can largely manage communication with the insurer and obtaining consent for certain courses of action. This does not absolve the insured from its obligations, but it can alleviate some of the burdens that would otherwise be solely on the insured when using non-panel vendors.

Will an insurer agree to retaining a vendor of our organization's choosing?

It depends. Insurers typically will not agree to off-panel assignments unless the policy contains language permitting such selection. In those instances, an insurer will still need to evaluate the vendor's qualifications, agree to an hourly rate, and require the vendor to comply with the insurer's guidelines for billing and reporting.

If an insurer consents to the retention of a vendor that is not on its panel, there will often be a difference in the hourly rate that is being charged by the firm and what will be agreed to by the insurer. That hourly rate difference will have to be borne by the insured.

What types of events should be reported to cyber insurers?

Insured organizations should report to insurers any actual or suspected security incidents, including ransomware, business email compromise and irregular network activity, as well as any written demands, tolling agreements, arbitration demands, regulatory inquiries and complaints. Written demands can include text messages, emails and communications in messaging apps.

If in doubt, contact Lockton. We will work with you to determine your reporting obligations.

Why should our organization retain a forensic accountant for the business interruption claim when we have a finance department?

Preparing and presenting an insurer with a proof of loss for business interruption as a result of a covered cyber event is a highly specialized and technical process. The types of losses presented must be the losses contemplated for cover by the policy. Not all claimed business interruption expenses and losses are covered.

Using a forensic accountant to prepare the proof of loss gives your organization the best chance for a successful resolution to your claim. A forensic accountant will also be better able to respond to the insurer's questions regarding any claimed losses.

Why is it necessary to retain legal advisors to investigate an information security incident before retaining other vendors, such as forensics?

Many organizations choose to retain legal advisors before retaining any other vendors, as some communications between organizations, attorneys and vendors during the course of an investigation may be legally protected from discovery in litigation.

What if my organization wants to work with a specific legal advisor and/or vendor?

The best course of action is to engage your cyber broker early and to discuss the possibility of adding vendors of your choosing (by endorsement) to a policy. Insurers will only consider endorsing vendors with significant expertise and at rates that are comparable to the rates paid to their panel vendors.

The Lockton claims difference

Managing a cyber claim can be difficult, complex and time-consuming. Tensions between insured organizations and other parties involved in the claims process — including insurers — can quickly become strained, which will only make the claims process more difficult and could prevent a successful resolution. For this reason, it's important to engage experienced claims professionals early.

Lockton's claims team provides guidance and claims advocacy support when our clients make cyber insurance claims. If there are questions regarding whether a matter should be reported under a cyber policy, Lockton's claims professionals can advise you and assist with reporting. If an insurer takes a questionable coverage position, Lockton's claims advocates are able to identify weaknesses in the insurer's coverage position and assert arguments supporting coverage. Lockton can also assist with introductions to panel firms and vendors, helping establish good working relationships from the start and enabling more favorable outcomes.

Lockton's Global Cyber & Technology Practice

As the world's largest privately owned, independent insurance broker, Lockton's independence gives us the freedom to be a strong, flexible advocate always acting in the best interest of our clients, creating an entirely different dynamic — one that's focused on your success. Led by a premier team of cyber brokers and advisors, Lockton's Global Cyber and Technology team is dedicated to delivering unparalleled service and innovative programs for your organizational needs.

Supported by cyber claims experts, former security practitioners and legally qualified technicians, our global team offers a wide range of expertise in risk identification, protection and management, as well as proven delivery of results.

Our global reach ensures that our clients have access to the knowledge that comes from experiences across multiple jurisdictions and industries.

$2.16B	65,000+	97%
2021 GLOBAL REVENUE	CLIENTS WORLDWIDE	CLIENT RETENTION

This playbook is for education and informational purposes only.
For assistance with your specific circumstances or for more information, please contact cyber@lockton.com.

UNCOMMONLY INDEPENDENT

C | 0718-1540027