Innovation Growth Partners Specialty®

CONTACT US

Dave Perkins, RPLU
(508) 848-4263
dave.perkins@igpspecialty.com

Best Practices:
Notifying a Cyber Insurance Carrier of a Cybersecurity Incident

From both a coverage and claims-management perspective, the safest approach is to notify the cyber insurer as soon as there is a reasonable suspicion that a potentially covered cyber event has occurred, even if the full scope of the incident is not yet known. Delayed notice is one of the most common causes of coverage disputes.

Executive Summary

KEY RECOMMENDATION: Notify the cyber carrier early, notify in writing, and follow all policy-specific reporting requirements.

Organizations should:

1. Review the policy's notice provisions immediately.
2. Notify the carrier and broker promptly. (Call the cyber insurer's claims hotline immediately to provide initial notice and then submit a written notice in accordance with the policy requirements)
3. Engage approved breach counsel and forensic vendors when required.
4. Provide facts, not assumptions.
5. Document all communications and actions.
6. Continue updating the carrier as the investigation develops.

When Should Notice Be Given?

Generally, notice should be provided when:

- A ransomware attack is suspected.
- A business email compromise (BEC) event is discovered.
- Sensitive information may have been accessed, stolen, or exposed.
- Significant system outages occur due to malicious activity.
- A privacy complaint or regulatory inquiry is received.
- Extortion or ransom demands are made.
- A third party alleges that your systems caused harm to them.

BEST PRACTICE: If you are debating whether to report the matter, it is usually safer to notify the carrier and reserve rights under the policy than to wait for the facts to become clearer.

What Should Be Included in the Initial Notice?

The initial report does not need to contain all details. Most carriers understand that facts develop over time.

At a minimum include:

- Policyholder name
- Policy number
- Date and time incident was discovered
- Brief description of the event
- Known impacted systems
- Whether operations are disrupted
- Whether law enforcement has been contacted
- Whether any ransom or extortion demand has been received
- Primary internal contact information
- Request for assignment of breach counsel and claim resources, if needed

***Always** keep an offline/ hard copy of your Cyber Insurance Policy and Incident Response Plan with the Claim Reporting Instructions.*

Avoid:

- Speculating on root cause
- Estimating damages too early
- Admitting fault
- Making statements unsupported by forensic evidence

Engage the Carrier Before Retaining Vendors

Many cyber policies require or strongly encourage use of their Panel Vendors for the following:

- Breach counsel
- Digital forensic firms
- Crisis communications consultants
- Notification vendors
- Credit monitoring providers
- Ransom negotiators

Failing to obtain insurer consent before retaining expensive vendors can create reimbursement issues.

EXAMPLE:
A company discovers ransomware at 2:00 a.m.

BEST PRACTICE:

- Isolate affected systems.
- Call the cyber insurer hotline immediately.
- Contact the broker.
- Request appointment of breach counsel.
- Engage forensic resources through counsel or carrier.

This helps preserve insurance coverage and may also preserve attorney-client privilege.

Preserve Evidence

Before rebuilding systems or deleting data:

- Preserve logs.
- Preserve forensic images where possible.
- Document timelines.
- Capture indicators of compromise.
- Maintain records of business interruption.

Destroying evidence prematurely can complicate both the forensic investigation and the insurance claim.

Coordinate Internal Teams

The cyber insurer should not be receiving inconsistent information from different stakeholders.

Involve:

- IT/Security
- Legal
- Risk Management
- Insurance Broker
- Executive Leadership
- Communications Personnel

Establish a single point of contact for carrier communications (ocsecurityaudit.com, ir-os.com).

Ongoing Reporting

Cyber claims evolve rapidly. Following initial notice:

- Provide investigation updates.
- Report newly discovered affected systems.
- Track remediation costs.
- Maintain business interruption records.
- Submit invoices and proofs of loss promptly.

Good documentation typically improves claim handling and reduces disputes regarding covered loss calculations.

Common Mistakes That Can Jeopardize Coverage

1. Waiting for Complete Facts
Many organizations delay notice until they "know exactly what happened." By then, policy notice requirements may have been missed.

2. Notifying Only the Broker
Notice to the broker alone may not satisfy policy requirements unless the policy specifically permits it.

3. Hiring Vendors Without Carrier Approval
This may create disputes over reimbursement.

4. Paying a Ransom Without Consulting the Carrier
This can create coverage and regulatory complications.

5. Destroying Evidence During Recovery
Rebuilding systems before evidence collection may impair both claims recovery and the investigative process.

Recommendation

Organizations should provide notice to their cyber insurer immediately upon discovery of a potentially covered cyber incident, even if the investigation is in its early stages. Early notification allows the insurer to deploy breach counsel, forensic experts, and other response resources, while helping preserve coverage rights under the policy.

Policyholders should avoid making assumptions regarding cause or scope, maintain detailed documentation, preserve evidence, and obtain carrier approval before engaging outside vendors whenever possible.

©2026 Innovation Growth Partners Specialty, LLC | igpspecialty.com