Brown & Brown

CYBER INSURANCE

Cyber Breach Response: First Steps

When You Suspect a Breach, Every Minute Counts

Discovering a cyber breach, or even suspecting one, can feel overwhelming. You may not know what happened, who's responsible, or what to do next. What matters most right now is acting quickly and calmly. This guide gives you a clear, practical path forward.

Prepare Before a Breach Happens

The single most important thing you can do today is decide who to call before you ever need to make that call. When a threat actor is actively inside your systems, time spent searching for help is time they spend causing damage.

If you have cyber liability insurance (a policy that covers costs related to data breaches and cyberattacks): Your first call is to your insurance carrier. Your carrier connects you to a breach response coach and pre-approved specialists. You don't need to build a response team from scratch.

If you don't have cyber insurance: You need to identify your key response resources now and keep their contact information accessible to everyone who might need it. Don't wait until an incident forces the search.

First Steps When a Breach is Suspected or Confirmed

Act quickly, but don't act alone.

- **Call your cyber insurer first (if insured):** Your carrier activates your response team and guides your next moves
- **Alert your internal IT or security team immediately:** If you don't have one, move to your external incident response firm
- **Contain the threat:** Disconnect compromised systems from your network if you can do so safely, without deleting anything
- **Notify your legal counsel:** Attorney-client privilege can protect your breach investigation communications
- **Document everything:** Write detailed notes from the moment you notice something is wrong

What Not to Do

Panic can lead to costly mistakes. Avoid these:

- **Don't delete files, logs, or communications:** You may destroy critical evidence
- **Don't make public statements or notify customers yet:** Wait until legal counsel advises you
- **Don't pay a ransom without consulting counsel and your insurer:** Payment decisions carry legal, regulatory, and strategic consequences
- **Don't assume the threat is gone:** Threat actors often leave multiple access points open

Preserve Evidence

Your investigation, your legal position, and any regulatory response depend on what you can prove.

- Take screenshots or photographs of any suspicious activity or error messages you see
- Preserve system logs and don't allow routine automated deletion processes to run
- Write down the timeline of what you noticed and when, including names of anyone involved

Resources You'll Need

These four resources are critical in nearly every incident:

- **Cyber insurer:** Coordinates your response, helps cover eligible costs, and connects you to vetted specialists
- **Legal counsel (breach-experienced):** Advises on notification obligations, regulatory exposure, and liability (U.S. breach notification laws vary by state; also, if your business serves customers in other countries, you may need to comply with international privacy laws, such as the EU's GDPR)
- **Breach response coach:** Manages the overall incident response process and helps you prioritize decisions under pressure
- **IT or incident response firm:** Identifies how the breach occurred, removes the threat, and helps restore systems

Resources You May Need Depending on the Incident

The scope of your breach determines what else you'll need. Some examples include:

- **Privacy counsel:** Guides compliance with specific data privacy regulations, particularly if sensitive personal data, health records, or financial information was exposed
- **Communications support (PR or crisis communications):** Helps you manage messaging to employees, customers, vendors, and the media if public disclosure becomes necessary
- **Law enforcement (FBI or local authorities):** May be appropriate when criminal activity, ransomware, or national security concerns are involved
- **Regulatory counsel:** Advises on industry-specific reporting requirements, such as those tied to healthcare (HIPAA), financial services, or critical infrastructure

You Can Get Through This

Acting quickly, following a clear process, and leaning on specialty resources help improve recovery outcomes. The preparation you do today, knowing who to call and having that information ready, directly shapes how well you respond tomorrow.

Breach response requirements vary by jurisdiction, industry, and the specific nature of an incident. Consult qualified legal counsel and your insurance carrier for guidance specific to your situation.

For questions or support, contact your Brown & Brown representative or cyber@bbrown.com.

About Brown & Brown

Growth has no finish line. Our team is with you along your growth journey to help find solutions that meet your ever-evolving insurance needs. Whether you are a highly complex multinational enterprise, an individual or anything in between, our experienced teams can help to find solutions at every stage.

Brown & Brown

Find Your Solution at BBrown.com
