

# CYBER CLAIMS ROADMAP

With cyber incidents on the rise and constantly evolving, it's vital that a cyber policy is in place, and that the response process is clear in case of an incident. There are certain steps that must be taken to help ensure coverage will be there when needed.

**1** Your company has suffered a security incident. You're the victim of unauthorized access to your network. Or maybe you've had an attack perpetuated through malware, viruses, spyware, or the like. The clock is now ticking. A quick, effective response may help you avoid lawsuits and regulatory inquiries.

**2** Immediately gather your internal team and review your incident response plan. Quickly prep for reporting to your insurer. Important information to cover includes: What type of event was it? Is there a lost device? Malicious hacker? Disgruntled employee? What type of information was affected? Where are affected individuals located? How many people are involved?

**3** Your policy will have a cyber hotline typically monitored 24/7. Call it and get any necessary action started.

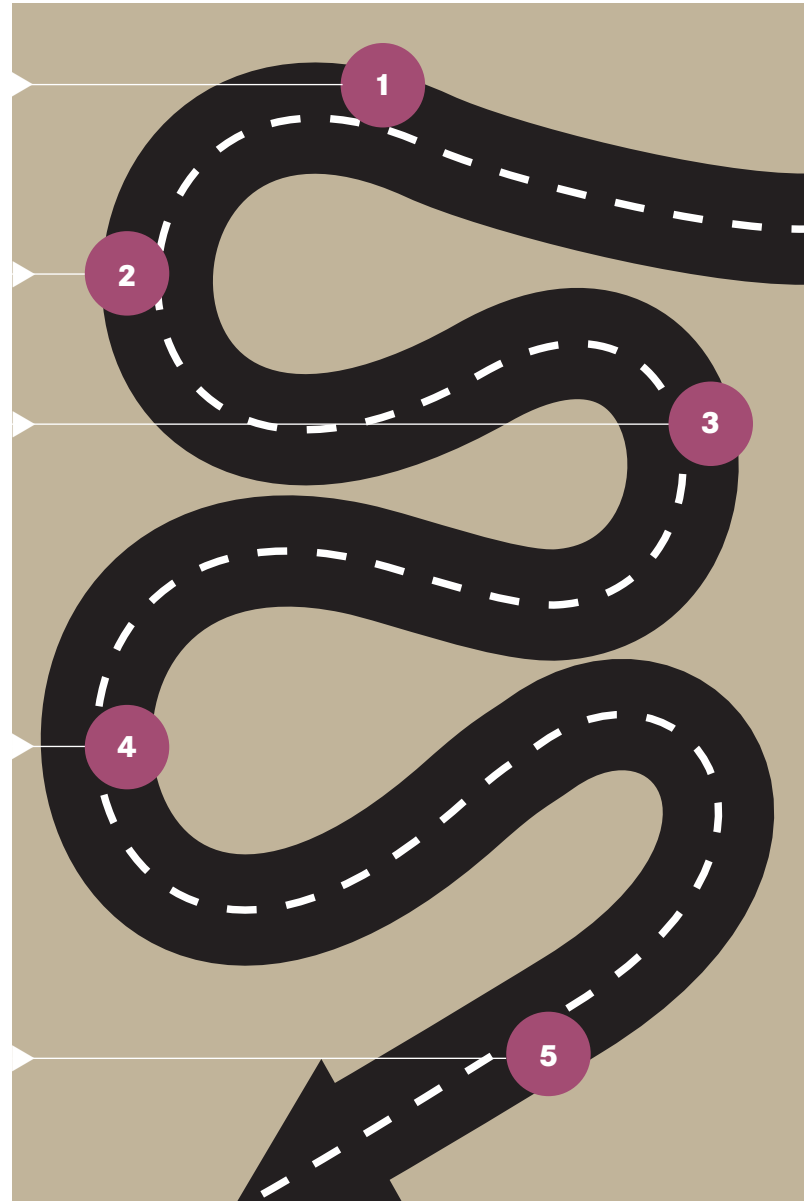
**4** Your claims specialist will help you formulate your response plan. It is critically important that you NOT go ahead and do these without contacting your insurer first. In most cases, the insurer and their vendors manage all aspects of the claims process.

Your response plan may include:

- engaging pre-approved expert privacy attorneys to determine legal applicability of actions to respond to reporting requirements and maintain privilege.
- engaging computer forensics to determine existence, cause and scope of the breach.
- engaging a public relations or crisis communications firm
- conducting proper notifications, which might include customers, employees
- setting up a call center
- providing credit or identity monitoring

**5** Your claims team will walk you through every step of responding to the incident and offer assistance and take actions on your behalf as necessary.

While this roadmap is intended as a guide, details for accessing each insurer's claims hotline service and instructions on how to notify a cyber claim are listed in each policy.



**Important! Do NOT go ahead and hire your own vendors. First: contact your insurer and breach attorney. Vendors not only have to be insurer approved, but they must be engaged through the attorney to maintain attorney-client privilege.**



## THE BOTTOM LINE

Understanding your organization's total cyber risk can be difficult, but the process can be greatly streamlined when assisted by a trusted insurance expert highly experienced in all the various forms of cybercrime and how to insure them. Preparation is key when it comes to cybercrime prevention and loss controls. Bringing an expert into the process as early as possible can help ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.