CYBER INCIDENT QUICK GUIDE

Gallagher

Insurance | Risk Management | Consulting

We take this opportunity to provide important information on the most urgent steps to be taken in the event that you suffer a cybersecurity incident, such as a ransomware attack or data breach:

1. **Immediately contact the cyber breach hotline** listed in your primary cyber insurance policy.
2. If you are experiencing a cybersecurity incident, including a ransomware attack, please be mindful of the following:
   - DO NOT communicate or negotiate with the threat actor before conferring with the breach coach.
   - DO NOT engage any vendor before speaking with the insurer representative or breach coach.
   - DO NOT incur any costs until after the initial conversation with the breach coach (which should be within a few hours from initial contact for live cyber incidents).
   - DO NOT wipe the infected machines, which risks losing the forensic artifacts that will be needed to investigate. If it is necessary to wipe the infected machines, ensure that you retain the necessary images before doing so.
3. Information requested in the initial call to the breach hotline typically includes:
   - Cyber policy number.
   - Some general information about your organization.
   - Details, to the extent known, regarding the cyber event (e.g., what happened, when the event occurred, when the event was discovered).
   - How the cyber event was discovered (e.g., internal discovery or contact from a customer, regulator or credit card company).
   - Whether the event appears to be contained or is potentially ongoing.
   - The type of data involved and the number of known or potentially affected individuals.
   - Whether or not there has been any contact with law enforcement; and

- Whether any party other than the insurer has been notified.
- Please note that prompt reporting of a breach or cyber incident is critical. Even if you do not yet have all the information listed above, please contact the insurer's breach hotline immediately if a breach is suspected.

4. Based on the initial information discussed, the breach coach will walk you through recommended steps to immediately be taken, which may include:
   - Retaining a forensic IT firm
     - » If you have already engaged a forensic IT vendor before calling the cyber breach hotline, that vendor's work should be billed as "Emergency Incident Response" and will need to be itemized.
   - Retaining a firm to negotiate a ransom with the bad actors, if necessary
   - Retaining other types of breach response vendors, if needed
     - These vendors will be engaged through the breach coach so that the attorney-client privilege and attorney-work product protections extend to the work of the forensic team and the ransom negotiator (which can be important in the event the client is later sued as a result of the cyber incident).
     - Many cyber policies require the use of vendor panel firms or the insurer's consent to the use of a non-panel vendor.
5. In addition to calling the cyber breach hotline, most cyber policies also require that formal written notice of the incident be provided to the insurer(s). Gallagher can assist in providing that formal notice — submit a request to GGBExecutiveCyberClaims@ajg.com.

If you do not report a cyber-related incident immediately, coverage could be jeopardized if the policy requirements are not met. This could leave you without coverage if unforeseen developments result in a claim or loss above the retention.

Connect with us

Cassandra C. Shivers Esq.
National Leader, Executive Risk & Cyber Claims
National Risk Control

Barbara S. Agulnek, Esq.
Team Leader, Cyber Claims Advocacy