Brown & Brown

PROPERTY & CASUALTY

Cyber War Exclusions in Focus

Iran Cyber Hostility

The most recent military engagements involving Israel, Iran and the United States have prompted heightened alerts from government agencies and the cybersecurity community. In March 2026, hackers aligned with Iran claimed responsibility for a significant cyberattack on U.S. medical device company Stryker, with the effects continuing to unfold. Reports also indicate Iranian-backed hackers are targeting data centers, industrial facilities, and airports in the Middle East.

Iran has a well-documented history of destructive cyberattacks. In 2012, Iranian actors deployed destructive malware against Saudi Aramco, disabling 30,000 computers and temporarily cutting the company's oil production in half. In 2024, Iranian hackers infiltrated the email system of the Trump campaign and reportedly targeted U.S. water plants and networks used by military and defense contractors. Since the most recent events, researchers at the cybersecurity firm CrowdStrike have detected a surge of activity from hackers from which may be related to Iran or acting in support of Tehran.

Cyber Insurance Response

War exclusions were not a prominent feature in most cyber policies until the NotPetya attacks in 2017 brought them into sharper focus. Exclusions were not raised by cyber underwriters in response to those attacks, but the event did serve as the impetus for an in-depth review of war exclusions. Since then, a broader and more nuanced range of exclusions has been developed.

Coverage for events connected to the conflict will depend on both the circumstances of the attack and policy provisions. Exclusions now fall into three broad categories.

1. Cyberterrorism carve-back clauses: These terms have a wide exclusion but incorporate a "cyberterrorism" carve-back and are being replaced. The exclusion will likely apply to actions arising from the current conflict, and the insured will rely on the carve-back for coverage. The application of the carve-back can depend upon:

   - The connection between the attacking group and the hostile parties
   - The motivation of the attacker (political, social, religious, or otherwise)
   - The connection between the attack and physical combat

2. Lloyds LMA Clauses: These clauses became widely accepted after Lloyds introduced them to the market. They exclude cyber events arising out of physical war while preventing coverage for cyber operations due to:

   - Available evidence of attribution to a hostile state
   - The impact of a cyber-attack on essential services in a target state
   - Whether the impact is "collateral" to the physical war

3

Company Clauses: Other carriers have crafted their own exclusions. A number of these have specific provisions which can provide greater clarity regarding the application of the exclusion. Elements in these clauses can have coverage depend upon:

- The formal declaration of war by a state
- Government authorities authorizing the use of force because of cyber-attacks
- Sanctions by international bodies because of cyber attacks

Governments are urging heightened cyber vigilance. As teams work through their objectives to remain secure, they should consider reviewing services provided by their cyber insurance provider. Companies should identify and develop relationships with their incident response service providers to proactively understand how they will combine as a team if a cyber event were to strike. A well-managed response can significantly diminish the impacts.

Brown & Brown has long supported organizations with comprehensive cyber policy provisions and war exclusions, continually adapting to address emerging threats. We are available to review your policy provisions and offer clear guidance to help ensure your coverage is effective in responding to attacks from Iran or its proxies.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com