MSV INSURANCE AGENCY

Cyber Risks & Liabilities

Taking a Closer Look at War Exclusions and Cyber Coverage

War exclusions are commonly found within commercial insurance policies. While these exclusions are fact-specific and often vary between policies and insurers, they generally state that damages from "hostile or warlike actions" by a nation-state or its agents won't receive coverage. Such exclusions were created to help protect insurers against systemic losses that may arise amid attacks by governments, their militaries or associated groups.

Cyber insurance policies are no exception to war exclusions. However, the rise of nation-state cyberattacks and growing international cyberthreats have posed questions regarding how these exclusions should be interpreted in the realm of digital warfare. In recent years, some court rulings have narrowed such exclusions for digital warfare; they emphasize that policy wording must specifically address losses stemming from nation-state cyberattacks in order for coverage restrictions to apply (i.e., Merck & Co. v. ACE American Insurance Co.).

In response to these rulings, insurers have made certain adjustments to protect themselves from facing unanticipated claims related to cyberwarfare. Primarily, insurers are being increasingly apprehensive in their selection of policyholders, thus utilizing more extensive application processes and requiring insureds to provide detailed documentation on their cybersecurity practices. Furthermore, insurers are exploring ways to ensure their policy language—namely, the wording within war exclusions—provides clear and consistent guidelines for what is and isn't covered, particularly in the scope of digital warfare.

As a result, it's critical for insurers and insureds to have open communication about policy definitions and specific coverage capabilities, especially as it pertains to protection against cyberwarfare. Such communication will help ensure both parties are on the same page, minimizing potential issues when claims arise.

Apart from fostering open dialogue with their insurers about coverage for losses due to digital warfare, it's also vital for insureds to take steps to prevent and mitigate these losses. These steps may include analyzing nation-state cyberattack exposures, engaging in incident response planning, leveraging adequate security software and following applicable government guidance. Such efforts could also reduce insurer apprehensions regarding obtaining coverage for damages caused by cyberwarfare. For additional insurance resources and solutions, contact us today.

Using Cyber Incident Response Planning to Limit Reputational Risks

Nearly half (46%) of businesses have faced reputational damages due to cyber incidents, according to a Forbes Insight Report. After a company experiences such an incident, its stakeholders may question its digital hygiene and data protection practices. Furthermore, these parties might lose confidence in the company's cybersecurity measures and privacy capabilities, resulting in lost funding and reduced customer loyalty. Cyber incidents can carry substantial reputational exposures, but response planning

can help businesses enhance their preparedness for these incidents and limit associated damages. In turn, companies' reputations can be upheld during incidents, demonstrating to their stakeholders that they can successfully navigate difficult circumstances.

Effective cyber incident response planning requires coordination across a company. A successful incident response plan should outline potential cyberattack scenarios as well as the methods and the individuals responsible for maintaining key functions during these scenarios. The plan should also be routinely reviewed to ensure effectiveness. Additionally, businesses should secure adequate cyber insurance. This coverage not only offers protection against financial losses that may result from cyber incidents but may also provide access to additional vendors and resources that can help companies effectively respond to such incidents, thus preventing associated reputational issues.

For further risk management guidance, contact us today.

Beware of These Top Phishing Scams

Phishing is a type of cyberfraud that utilizes deceptive emails or other electronic communication to manipulate recipients into sharing sensitive information, clicking on malicious links or opening harmful attachments. Many significant cyberattacks have included a phishing component. In fact, in its 2021 Data Breach Investigation Report, Verizon noted that phishing played a role in approximately one-third of all breaches analyzed. Here are some of the most common types of phishing scams:

- **Deceptive phishing**—Deceptive phishing is when a cybercriminal impersonates a recognized sender to steal personal data and login credentials. These emails often trick victims by asking them to verify account information, change a password or make a payment.
- **Spear phishing**—A spear-phishing scheme is typically aimed at specific individuals or companies and uses personalized information to convince victims to share their data. In these instances, cybercriminals will research a victim's online behavior—such as where they shop or what they share on social media—to collect personal details that make them seem legitimate.
- **Whaling**—Whaling aims to trick high-profile targets such as CEOs, chief financial officers and chief operating officers into revealing sensitive information, including payroll data or intellectual property. Since many executives fail to attend company security trainings, they are often vulnerable to whaling scams.
- **Vishing**—Vishing, or "voice phishing," occurs when a criminal calls a target's phone to get them to share personal or financial information. These scammers often disguise themselves as trusted sources, such as a bank or the IRS, and rely on creating a sense of urgency or fear to trick a victim into giving up sensitive information.
- **Smishing**—Smishing refers to "SMS phishing" and incorporates malicious links in SMS text messages. These messages often appear to be from a trustworthy source and lure victims in by offering a coupon code or a chance to win a free prize.
- **Pharming**—Pharming is a sophisticated method of phishing that redirects a victim to a site of the cybercriminal's choosing by installing a malicious program onto their computer. The goal is to have users input their login credentials or personal information, such as credit card numbers, on the fraudulent site.

As more criminals turn to online scams to steal personal and company information, business leaders must remain vigilant in their cybersecurity efforts. These efforts may include hosting robust employee cyber training, equipping workplace devices with sufficient antivirus software and conducting routine data backups. Through such measures, businesses can stay protected against a range of phishing threats.