Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A New Obstacle For Cyberinsurance Coverage

Law360, New York (September 06, 2013, 12:14 PM ET) -- As the recent spate of cases and news stories confirms that the rising threat and costs of cyberattacks have become a painful reality for U.S. and global companies and institutions. In 2012, cyberattacks against U.S. businesses increased by an estimated 42 percent, while over 90 percent of large U.K. organizations suffered on average 113 cyberattacks in 2012 alone.

Cyberattacks are estimated globally to cost nearly $400 billion annually (including downtime caused by the attacks). In addition, cyberattacks cost U.S. entities an estimated $250 billion annually in lost intellectual property. Victims have included every major U.S. bank, major defense contractors and even Google.

As a result, more and more companies have been asserting cyber-related claims under commercial general liability (CGL), business interruption and other noncybersecurity policies and seeking specific first and third-party coverage against cybersecurity breaches. As the case law concerning cyber risks slowly develops, and a market for cybersecurity coverage grows, a new wrinkle for cyberinsurance is emerging that may create additional bars to coverage for attack victims and present novel evidentiary issues for insurers.

Intrusions and data breaches are not just caused by criminals and individual hackers. Instead, a growing body of evidence indicates that the most destructive and costly cyberattacks are the result of cyberwarfare directed by state actors and terrorists. This poses a significant problem for companies seeking coverage for losses arising from cyberattacks because the war and terrorism exclusions commonly found in cybersecurity and CGL policies bar recovery for such losses.

This is especially true following the decision in In re September 11 Litigation, which could expand the scope of the war exclusion. At the same time, insurers face their own potential issues, including establishing both “who did it” and whether the attack or hack was an act of clandestine cyber espionage or warfare.

Attacks in Cyberspace May Constitute Acts of War

Developments in cyber technology have fundamentally changed war-fighting, espionage and business competition. The United States has officially classified cyberspace as a fifth “domain” of warfare, alongside land, air, sea and space.

In 2010, the U.S. Department of Defense established the U.S. Cyber Command to conduct cyber-warfare operations, protect cyber infrastructure, and counter threats in cyberspace — the “battlefield of the 21st century.”

As former Secretary of Defense Leon Panetta remarked, “There is a strong likelihood that the next Pearl Harbor that we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems.”

The United States is not alone. All major world powers have established their own cyberwarfare capabilities to acquire information, manipulate and override infrastructure systems, damage computers and networks, release viruses, probe weaknesses in opponents’ data and network security and steal intellectual property. Many countries today engage in an ongoing “soft” cyberwar targeting governments and companies in other countries.

The Ongoing Soft Cyberwar

While the U.S. has not experienced a cybersecurity Pearl Harbor event to date, the public and private sector in the U.S. and its allied countries currently suffer from the rising onslaught of cyberwarfare from multiple aggressors. This cyber “soft war” or “cold war” has typically been waged in secret to avoid detection and attribution.

Attackers deploy various techniques to intrude upon computer and network systems, usually to steal information covertly. The loss of intellectual property to government-supported cyberattacks has been declared the largest illegal wealth transfer in world history.

According to industry and news reports, Unit 61398 — the cyber unit of China’s People’s Liberation Army — has attacked hundreds of companies around the world, including Coca-Cola Company, RSA (a maker of data security products used by U.S. governmental agencies and defense contractors), Lockheed Martin, oil and gas pipeline companies, chemical plants, mining companies and satellite and telecommunications corporations. Approximately 90 percent of all cyberespionage in the U.S. reportedly originates in China.

In its recent report to Congress, the U.S. Secretary of Defense, for the first time, attributed intrusions and cyberattacks to the Chinese government and its military. The U.S. government’s recent statements concerning China mark a shift in the cyberwarfare landscape — formal recognition by the U.S. government of a foreign sovereign and its military using cyber weapons against the U.S. in a deliberate, government-developed strategy to exfiltrate intellectual property and other strategic information.

China is not the only country conducting cyberwarfare against private businesses. North Korea’s cyber unit has conducted attacks against banks and media outlets. Iran has launched cyberwarfare against Israeli targets and energy companies and — through a terrorist organization, Izz ad-Din al-Qassam Cyber Fighters — has also reportedly directed attacks on America’s financial institutions, including Bank of America, JPMorgan Chase, Citigroup and Wells Fargo.

These attacks have targeted the banks’ networks, causing intermittent delays, systems to be taken offline and functional damage to their online services.

In addition to state actors, terrorist organizations are also attempting to conduct cyberwarfare. For example, in 2011, al Qaeda called on its members to conduct cyberattacks against Western targets.

Losses and Market Developments

The financial risks imposed by cyber threats are significant. The average cost of a data breach for a U.S. company is nearly $9 million. Every minute of disrupted service to a U.S. bank’s website is estimated to cost the bank $30,000. One of the largest cyberattacks to date occurred against Sony in 2011. The attacks cost Sony an estimated $1 billion to $2 billion.

The rapid increase of these cyberattacks and resulting losses have created substantial potential exposure for insurers and reinsurers. To manage this exposure, insurers have sought to shift cyber risks to specific cyber or information security endorsements and policies by including cyber or electronic data exclusions in CGL and other policies and construing losses from cyberattacks as outside the scope of insuring clauses and damage definitions.

The market for cybersecurity policies — especially with higher limits — is still developing, however, due to significant underwriting challenges. The U.S. Department of Homeland Security has even established cybersecurity insurance working groups to "determine what obstacles prevent carriers from offering more relevant policies to more customers at lower cost and promote stakeholder discussion about how to move the cybersecurity insurance market forward." As a result, noncyber-specific policies still present insurers with potential exposure and thorny legal questions.

As evidence increases that state actors or terrorists are conducting attacks, one possible limitation found in both cybersecurity and noncyber-specific policies are the war and terrorism risk exclusions.

War and Terrorism Risk Exclusions

The war and terrorism risk exclusions may effectively limit insurers' exposure to many costly and high-profile cyberattacks. Most traditional CGL, property and business interruption policies include an exclusion for losses related to war. Insurance Services Office's cybersecurity insurance policy form (information security protection policy) also includes a war risk exclusion.

Although the language within policies varies widely, the war risk exclusion generally excludes injuries caused by or arising, directly or indirectly, out of war, including undeclared or civil war; warlike action by a military force; and insurrection, rebellion, revolution, usurped power or action taken by governmental authority in hindering or defending against any of these.

Traditionally, courts interpreted "war" and "warlike actions" as events involving two sovereigns or quasi-sovereign governmental entities. In the absence of direct involvement by a sovereign state, the war risk exclusion historically did not apply to bar coverage.

For example, in the context of the Pan Am attacks in 1973 by the Popular Front for the Liberation of Palestine, the Second Circuit rejected the insurers' position that the war risk exclusion applied to deny claims arising from those attacks. See Pan Am. World Airways Inc. v. Aetna Cas. & Sur. Co., 505 F.2d 989 (2d Cir. 1974).

The court held that war required the hostile engagement of a sovereign or quasi-sovereign nation. Id. The court concluded that terrorist acts against civilians by operatives of a political organization or guerilla group cannot be characterized as war or warlike operations. Id. This narrow interpretation of the war exclusion traditionally limited the scope of its application.

Cyberattacks from the ongoing soft cyberwar, however, likely satisfy even this restrictive requirement of a sovereign or quasi-sovereign actor. Cyberattacks are now doctrinally understood by the U.S. Department of Defense as military operations or warlike actions, and cyberattacks brought by or at the behest of the Chinese government or military, Iran's government or some other country's government are brought by a sovereign or state actor.

Moreover, the narrow reading of the exclusion may loosen as a result of the recent opinion in In re September 11 Litigation, 2013 U.S. Dist. (S.D.N.Y. March 20, 2013). The court in In re September 11 Litigation determined that the "act of war" exception to Comprehensive Environmental Response, Compensation and Liability Act liability applied to claims stemming from 9/11.

In construing the statute's act-of-war clause, the court distinguished the Pan Am decision and insurance-related precedent requiring a state actor to conduct war. The court found that the elaborate and well-planned 9/11 attacks were carried out by an extra-national terrorist organization that had declared war on the United States and intended to bring down its leading commercial and political institutions.

The court recognized that warfare is often waged by irregular forces capable of causing extraordinary damage. As such, and because of the United States' response to 9/11, the court concluded that the 9/11 attacks constituted acts of war.

The expansion of the war risk exclusion to encompass irregular forces or terrorists could aid insurers seeking to limit cybersecurity losses. Following the $40 billion in losses arising from 9/11, insurers and reinsurers issued terrorism exclusion endorsements to their outstanding policies and included them within new policies.

As with war risk exclusions, the language of terrorism risk exclusions varies. Since the passage of the Terrorism Risk Insurance Act (TRIA), many terrorism risk exclusions bar recovery for injuries or damages arising, directly or indirectly, out of acts of terrorism as determined or "certified" by the secretary of U.S. Treasury.

The secretary, however, has never certified a cyberattack as an act of terror. In fact, in its first test of its certifying authority — the April 2013 Boston Marathon bombings — the secretary has yet to classify the attack.

Not all terrorism risk exclusions, however, are tied to the secretary of Treasury's certification process. Some exclusions preclude coverage for noncertified terrorists events. These exclusions are likely much more powerful in limiting exposure to cyberterrorist attacks.

Insurers looking to rewrite their terrorism risk exclusions — especially in the face of uncertain prospects for TRIA's renewal beyond its Dec. 31, 2014, expiration — should consider excluding noncertified terrorist events.

Evidentiary Challenges Facing Insurers

Neither the war nor terrorism risk exclusions represent perfect solutions for insurers for mounting cybersecurity losses. First, the exclusions were not written with cyberattacks in mind, and the language could more specifically identify cyberwarfare.

Second, insurers typically bear the burden of proving that exclusions apply. Thus, insurers may face the challenge of proving "who did it" in seeking to rely on either a war or terrorism risk exclusion.

During the ongoing soft cyberwar, perpetrators typically deny involvement. The recent position taken by the U.S. government with respect to China, and to a certain extent, Iran, helps insurers immensely.

Still, because cyberattacks are a recent phenomenon, it is not entirely clear what types and level of proof courts will require insurers to show in support of coverage declinations. At a minimum, it appears proof will require sophisticated Internet and computer forensics and the assistance of cybersecurity companies.

As evidence continues to point to cyberwarfare being committed against insureds, insurers should investigate claims seeking coverage for cybersecurity breaches carefully to determine whether a war or terrorism exclusion might apply. In conducting such an investigation, insurers may, in appropriate circumstances, want to consider retaining sophisticated cybersecurity companies.

In addition, insurers may want to consider whether their existing war and terrorism exclusions are sufficient to exclude coverage for claims arising from cyberwarfare conducted by nation states or terrorist organizations.

--By Peter Bryan Moores and Samantha Krasner, Choate Hall & Stewart LLP

Peter Bryan Moores is a partner, and Samantha Krasner is an associate in the insurance and reinsurance and major commercial litigation groups at Choate Hall & Stewart in Boston.

The opinions expressed are those of the author and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.
