January 2019

Alert: How Cyber Terrorism Could Impact Your Insurance Coverage

NotPetya, WannaCry, and countless cyber hacks on both public, private and government organizations alike have led some of the most powerful nations to point fingers – at each other. Cyber-attacks and breaches of network security are nothing new. However, the breadth and severity of certain cyber-attacks have led to accusations of cyber terrorism against specific governments and countries. But where you, the insured, is concerned – why does it matter whether the cyber-attack that wreaked havoc on your business is labelled as 'cyber terrorism'? It matters because whether a cyber security incident is classified as cyber terrorism can potentially affect the coverage available under your insurance policy.

Cyber terrorism insurance litigation

Mondelez, the candy manufacturing giant, was a victim of the global NotPetya malware attack in June 2017. The virus disabled and allegedly caused permanent damage to 1,700 of the company's servers and 24,000 laptops. The company also claimed theft of user credentials, unfulfilled customer orders, and other losses – altogether, damage estimates topped $100 million. Mondelez claimed the loss under its property insurance policy, which provided coverage for (1) "physical loss or damage to electronic data, programs or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction," and (2) "interruption directly resulting from the failure of electronic data processing equipment or media resulting from malicious cyber damage." In June 2018, Zurich, the insurer, denied coverage on the basis of an exclusion contained in the policy, which precluded coverage for loss from "hostile or warlike action in time of peace or war... by any government or sovereign power, military, naval or air force, or agent or authority of any party specified above." The two parties have since been locked in an ongoing coverage dispute. Notably, in February 2018, the UK government publicly attributed the NotPetya attack to Russia. Similar official statements from other nations followed, including the U.S. As the burden of proof laid with Zurich to show that the exclusion applied to preclude coverage, the insurer has pointed to these statements in support of their position that the 'terrorism' exclusion applies.

Cyber-attacks are notoriously difficult to attribute to a particular party, and the associated motives behind the attack are equally hard to prove. This can lead to coverage uncertainty, as evidenced by the Mondelez-Zurich dispute. This litigation undoubtedly raises many issues, both legal and insurance-related, and will surely result in a precedent-setting decision with implications for insureds across North America. However, a very important issue remains –Mondelez was seeking cyber coverage for certain losses under its property insurance policy, which provides more limited cyber coverage compared to a dedicated cyber liability insurance policy.

Cyber liability insurance

The vast majority of property and commercial general liability policies contain a 'war' or 'terrorism' exclusion, such as the one contained in Mondelez's property policy, and furthermore were not designed with the intent of providing robust cyber coverage. While most cyber insurance policies also contain a form of this exclusion, it is market standard for the war/terrorism exclusion to be carved-back to allow coverage for cyber-terrorism related risk exposures, including state-sponsored cyber-attacks. In this vein, a cyber liability insurance policy can provide protection in the event you are a victim of a hack or malware virus potentially initiated by a state-sponsored actor. In addition, a cyber liability insurance policy can provide the following robust coverage:

Coverage	Cyber insurance
Privacy/cyber breach (actual or alleged) response costs, including: • Dedicated breach response team of experts, including legal counsel, providing 24/7 on-call support • Breach notification expenses, including the cost of hiring legal counsel and public relations consultants • Credit monitoring/protection costs • Notification and establishment of a call centre • IT forensic investigation costs • Identity theft resources • Proactive crisis management initiatives in the event of a suspected cyber breach	✓
Business interruption costs resulting from a network security failure (i.e. lost income, expenses to get system back up and running, etc.)	✓
Data restoration costs in the event of damage or alteration of intangible property (i.e. cost to restore/recreate data or software that is altered/destroyed by a network security failure)	✓
Cyber extortion costs (i.e. the amount of any ransom paid; cost to hire experts to assist in resolving the situation) Defence costs, judgment and/or settlement amounts for actions seeking damages as a result of wrongful disclosure of personally identifiable information or confidential corporate information in the firm's care, custody or control via a computer network or off-line (e.g. via laptop, paper, records, disks)	✓
Defence costs, judgment and/or settlement amounts for actions seeking damages as a result of a failure of the insured's computer network security to guard against threats such as hackers, viruses, worms, Trojan horses and denial of service attacks	✓
Defence costs, judgment and/or settlement amounts for content liability perils such as actions alleging defamation and infringement of intellectual property rights arising out of website, marketing and advertising activities	✓
Defence costs for regulatory proceedings arising out of a security or privacy breach and coverage for administrative fines and penalties, where insurable	✓

Aon's integrated approach

The cyber liability insurance market is one of the most specialized in the world of commercial liability. Appropriately combining this coverage with a comprehensive property and general liability insurance program is a complex task that requires a sophisticated understanding of each policy form. As such, we recommend working with a broker that has extensive experience and a good understanding of the risk transfer solutions that are available. In addition to placing insurance across all major coverage lines, Aon has an integrated National Cyber & Privacy Practice composed of specialized brokers, account executives, lawyers and information technology professionals. Our brokers understand that few privacy and security risks are alike, and organizations have unique needs depending on their size, location, use of technology and the type of legal work performed.

Prepared by

Jessica Foster J.D.
Legal Consultant
+1.416.868.5651
jessica.foster@aon.ca

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.