Fine Print Online
May 2014

Mitigating Business Interruption Exposures from Cyberattacks

by Robert M. Horkovich and Marshall Gilinsky

What would happen to your business if a cyberattack disrupted online communications or transactions, shut down local or regional transportation, or caused a power outage? Fortunately, to date, relatively few of the technology-based risks have resulted in such serious problems or losses. It also is fortunate that insurance companies are offering new insurance products tailored to address a wide array of emerging risks – many with manuscripted wordings. Businesses of all shapes and sizes should carefully consider the impact a cyberattack would have on their operations and business income and take steps to make sure that their insurance will respond as desired.

It is not difficult to imagine the business interruption consequences of a direct breach of your company's computer infrastructure. But many companies face an equally large disruption to their business from a cyberattack on someone else – especially the transportation, banking, communications and energy industries. For example, what if your computer system or data are protected, but a hacking event shuts down the internal networks, power grid or transportation? Such events could lead to widespread business interruption losses in all sorts of industries. But are such losses covered under your insurance program?

Historically, property and business interruption policies required "direct physical loss or damage" to property in order to trigger business interruption coverage. Although the circumstances of a cyberattack surely could involve such loss or damage, some insurance companies might argue that they do not. Accordingly, savvy brokers and policyholders seek out policy wordings that unambiguously provide that business interruption coverage is triggered even in the absence of "physical" loss or damage.

Some property insurance policies require damage to the policyholder's own property or to property within a certain distance of an insured location in order to trigger business interruption coverage. Other polices offer much broader "contingent business interruption" coverage, which kicks in so long as there is damage to property of the policyholder's customers or suppliers, even customers and suppliers twice removed. Given the nature of the risks involved in cyberattacks on transportation, internet or power networks, it makes sense for policyholders to seek out policy wordings that clearly provide business interruption coverage when damage or disruption to such networks impacts the policyholder's business – even though the damage or disruption does not involve property at or near the policyholder's premises.

Finally, policyholders should consider the potential interplay between cyber and terrorism risks and ensure that losses from cyberattacks are covered and not excluded. As many cyberattacks originate from undefined locations and arguably are intertwined with political motives, the possibility exists that a large cyberevent could be deemed an act of terrorism. Accordingly, policyholders might consider seeking policy wordings that use "malicious damage" as a trigger of coverage, which would prevent the insurance company from avoiding coverage in the event that the U.S. government either did or did not certify a situation as a terrorist event. Under "all risk" insurance policies, all perils are covered unless specifically excluded. Policyholders should carefully review all of

the exclusions in their policies – especially the ones added via endorsements – to confirm that there are no hidden traps that could jeopardize coverage where a loss arguably involves an act or terrorism or cyber warfare.

Policyholders ought to be prepared for a catastrophic attack scenario. Carefully selected insurance policies can provide the greatest certainty for policyholders in the aftermath of such a loss event and give those policyholders a leg up in maintaining and rebuilding their businesses following the loss. After all, that is what business interruption insurance is designed to do. Given the extent of the damage that a cyberattack could cause, businesses need to make sure that their business interruption coverage is designed to respond in the event of such losses. ■

Robert M. Horkovich *is managing partner and shareholder in the New York office of Anderson Kill. He is a trial lawyer who has obtaining more $5 billion in settlements and judgments for policyholders from insurance companies.*

Marshall Gilinsky *is a partner in the firm's Washington, D.C. office. His practice is focused on property insurance, commercial general liability insurance, directors' and officers' insurance, captive insurance and reinsurance issues.*

RISK MANAGEMENT