Does Traditional Coverage Apply When Cyber Attacks Cause Physical Damage?

This article was originally published in the 2016 edition of *Claims Magazine*, a *PropertyCasualty360* publication.

by Alex J. Lathrop

Alex J. Lathrop
Litigation
+1.202.663.9208
alex.lathrop@pillsburylaw.com

Alex J. Lathrop is a partner in Pillsbury's Litigation and Insurance Recovery & Advisory practices. He has assisted clients with large, complex losses in a wide array of industries – ranging from energy, oil and gas, railroad and large manufacturing companies to emerging internet, technology and medical device companies.

A recent event that received surprisingly little media attention serves as a reminder of a lurking cyber risk that is different in kind and scale than more widely and frequently reported privacy-related data breaches. Between July 29 and September 14, 2016, **a series of fires and explosions occurred** at petrochemical plants and pipelines in Iran. Although Iranian government officials initially denied that the fires were caused by a cyber attack, they later acknowledged that Iran's petrochemical industry has been the target of cyber attacks, and the head of a cyber security firm specializing in protecting industrial systems stated that he was "100 percent" sure that the fires were the result of hacking.

Unlike more common data breaches, which result in disclosure of private information to an unauthorized third party, these cyber attacks were simply intended to cause damage more like large-scale vandalism. Costs associated with data breaches are generally covered under cyber insurance. But what about a cyber attack that causes physical damage and business interruption on a catastrophic scale? That is not the type of loss ordinarily covered by most cyber insurance policies. Such losses may, however, be covered under the broad language of a company's traditional property policies.

The Growth of Cyber Insurance

Over the past decade, privacy-related data breaches have become more frequent. When early data breaches were reported, such as TJX/TJ Maxx in 2007, they were a relatively unknown and anomalous phenomenon. Today, nearly every big business has experienced either an actual or attempted data breach. Typical costs associated with these data breaches include detection, investigation, notification, crisis management, legal defense, identity protection services, product discounts, and a host of other direct and indirect costs. According to a leading industry report, the average total cost to a U.S. company of a data breach in 2014 was $6.5 million.

As the risk of data breaches has grown, so has the market for cyber insurance. But while cyber policies are an important part of a company's risk management strategy, the market is relatively new and the policies have a number of limitations.

First, insurance industry representatives admit that cyber insurance capacity (i.e., the total amount of insurance available in the market) is

small compared to insurance markets covering other property and casualty risks. Limited capacity means a higher cost per dollar of insurance. Moreover, the amount of cyber insurance limits offered to particular insureds is relatively small in comparison to the property and casualty limits they typically buy.

Consider in 2015, companies with revenues over $5 billion bought on average $34 million in cyber insurance limits compared to over $500 million in property limits. And, cyber insurance policies ordinarily exclude losses arising out of property damage (and bodily injury). Finally, while many cyber policies will provide coverage for business interruption caused by a cyber attack, any such coverage necessarily is limited to the often relatively small amount of cyber limits the company purchased.

Cyber Attacks Causing Physical Damage

Although less publicized than privacy-related data breaches, there have been a handful of cyber attacks where hackers have accessed the process control systems of large industrial companies in order to cause a malfunction, resulting in property damage and a disruption of the company's operations. While these attacks have occurred with far less frequency than data breaches, the resulting loss from such an event could be catastrophic – far greater than the average loss associated with a data breach, and likely in excess of the amount of cyber insurance limits purchased by most companies. In addition to the recent Iranian petrochemical plant fires discussed previously, examples of such attacks include the following:

- In December 2015, over **80,000 people in the Ukraine lost power** when hackers infiltrated two power distribution companies' control systems and disconnected electrical substations. The hackers also attacked the utility company's service helpline, preventing customers from reporting the outage.
- In late 2014, hackers infiltrated the control system of a **German steel mill**, initially installing malware on the mill's computer systems, and then manipulating the control system to cause numerous individual components and systems to fail so that a blast furnace could not be properly shutdown, resulting in reportedly massive damage.
- Earlier this year, a hacker was charged by federal prosecutors with illegally gaining access to a computer system that controlled the **Bowman Avenue Dam** in Rye Brook, New York, in 2013. The hacker gained access to the dam's industrial control system, where he was able to control the computer that opened and closed the dam's sluice gates. Fortunately, there was no resulting property damage (other than to the computer system itself), as the sluice gates had been manually disconnected from the control system due to maintenance issues.
- In 2010, a computer worm known as **Stuxnet** was used to sabotage centrifuges in Iran's Natanz nuclear facility. The Stuxnet virus manipulated the computer systems that control and monitor the speed of the centrifuges, causing the centrifuges to speed up and slow down, ultimately destroying 1,000 to 2,000 of them.
- In 2008, hackers accessed the industrial control system of a **Turkish oil pipeline** and super-pressurized the crude oil until the pipeline exploded. The explosion caused more than 30,000 barrels of oil to spill into an area above a water aquifer. To facilitate the attack, the hackers preemptively shut down the alarm system designed to trigger the system's safety mechanism.

It is not difficult to imagine the wide ranging losses that could result from these sorts of cyber attacks, including destruction of a company's plant and equipment, damage to third-party property, and substantial losses of revenue while operations are interrupted. Whether these losses will be covered under a company's traditional property policy ultimately will depend on the specific language of the policy or policies purchased by the company.

Coverage Under Traditional Property Policies

Many companies buy "all risk" coverage, which covers loss resulting from any peril that is not specifically excluded. Thus, coverage will turn on whether the policy contains specific exclusionary language for cyber attacks, or applicable sub-limits or other limitations. While standard form property policies exist, the larger a company is, the less likely it is to purchase such standard form coverage.

The language in property policies purchased by large industrial companies, such as energy, oil and gas, mining, chemical, transportation and manufacturing companies, will often vary depending upon the industry, broker, insurer, length of the company's relationship with the underwriter, and numerous other factors. These companies do not buy generic form policies, instead choosing to buy manuscript policies that cobble together language insurers take from a variety of different forms. Given this relative lack of standardization in the property market, it is unlikely that language drafted by insurers specifically intended to exclude coverage for cyber-related losses has been adopted in a uniform manner or will be in the near future.

It is important for companies facing the potentially enormous risk of physical damage and business interruption caused by a cyber attack — particularly large energy, infrastructure, resource and manufacturing companies — to understand that their property policies may provide a source of recovery in the event of such a loss.

Yet even if these losses fall within the language of the policy, it is uncertain whether insurers will willingly pay such claims. On the one hand, the insurance industry has recognized that cyber attacks causing physical damage and business interruption are covered under traditional insurance products.

Notably, a **November 2015 report from A.M. Best on cyber security issues facing insurers** acknowledges that such claims are currently covered under the language of traditional insurance products such as commercial general liability, property and business interruption polices. However, the report states that the language in these policies was developed at a time when cyber liability claims were not contemplated.

This claim is specious. As insurers agree to renew their policyholders' property and business interruption coverage programs without explicitly addressing cyber-related losses, they cannot reasonably claim to be unaware of the risk they are taking on at the time of underwriting.

Another more striking acknowledgment of coverage under traditional policies for physical damage and business interruption losses caused by cyber attacks appears in a 2015 report jointly published by Lloyd's of London and the University of Cambridge's Centre for Risk Studies entitled, "**Business Blackout, The Insurance Implications of a Cyber Attack on the U.S. Power Grid.**" In that report, the authors consider the types of claims that could be triggered by a hypothetical disruption to the U.S. power grid resulting from a cyber attack.

The report acknowledges that physical damage resulting from such an attack would trigger first-party property damage and business interruption policies. Like the A.M. Best report, the Lloyd's report suggests that coverage for these attacks under traditional policies may not be intended, but concedes that many policies are "silent" or ambiguous as to whether such claims are included. The Lloyd's report refers to policyholders' expectation that such claims will be covered under their traditional policies and the belief by insurers that they are not as a "mismatch of expectation and reality."

But given the significant amount of attention cyber risk has received by the media, government agencies, insurers, brokers and policyholders, it would be unreasonable for insurers to believe that losses due to cyber attacks are not covered under traditional lines of coverage if they are not clearly excluded.

The admission by one of the largest excess insurers in the world that (1) policyholders and insurers do not share a common understanding of whether their traditional policies provide coverage for cyber-related losses causing physical damage, and (2) many such policies are silent on this issue, are particularly significant. As a practical matter, this means that coverage for such losses likely will be disputed, and the issue of whether the policies apply will either be compromised by the parties or decided by the courts. The role of a court in interpreting an insurance policy is to find the common intent of the parties, as expressed by the language of the policies.

Generally, clear and unambiguous terms in an insurance policy are given their plain and ordinary meaning. However, where language is susceptible to more than one reasonable interpretation, an ambiguity exists. To the extent, as the Lloyd's report suggests, traditional property policies are "silent" with

respect to coverage for cyber-related physical damage losses, this leads to only two alternatives: (1) the clear language of the policies is broad enough to encompass such losses, or (2) the policies are subject to more than one reasonable interpretation, and therefore are ambiguous.

Under general principles of insurance interpretation, ambiguities are resolved in the insured's favor and in line with the insured's reasonable expectations. Thus, under either alternative, "all risks" policies that are silent with respect to coverage for cyber-related losses should be interpreted to cover them.

Insurers have begun to develop exclusions specifically designed to limit coverage for cyber events resulting in physical damage and business interruption. Examples include Institute Cyber Attack Exclusion Clause 380 (CL 380) and LMSA 3030, which have been designed to bar coverage for claims relating to cyber attacks that are committed with malicious intent or are deemed acts of war.

Given the continued softness in the property market, policyholders are well positioned to resist attempts by insurers to add such exclusions. To the extent these or other exclusions already have been added, under general principles of insurance interpretation, exclusions must be narrowly construed, and the insurer bears the burden to show that the exclusion is: (1) clearly and unmistakably stated, (2) subject to no other reasonable interpretation, and (3) applicable to the present case.