Recent attention on high-profile data breaches has overshadowed a potentially greater risk: cyber-attacks on energy companies causing physical damage and business interruption. Recent publicly reported cyber-attacks, including explosions at an oil pipeline and a steel mill, have highlighted the potential vulnerability of Internet-facing industrial control systems to hackers. Current cyber-policies were designed to cover the costs of privacy-related data breaches; they typically exclude coverage for property damage and offer insufficient limits to cover the magnitude of business interruption losses that energy companies face from a cyber-attack on their operations. While some insurers have begun to offer new cyber-insurance products covering property damage and business interruption, policyholders may already have this coverage under their traditional property policies. Hear from a petroleum refining company risk manager, an energy property broker, and an insurance coverage lawyer on whether and how traditional property insurance may cover this growing cyber-risk.
Notes

This file is set up for duplexed printing. Therefore, there are pages that are intentionally left blank. If you print this file, we suggest that you set your printer to duplex.
Bob Gefers is the US Downstream Energy and Power Property Practice leader in Marsh’s Houston office, which is part of the Energy and Power Practice. He serves as a client executive and is also involved in the design, marketing, negotiation, and ongoing service of major property programs for energy- and power-related companies.

Mr. Gefers joined Marsh in 2009. He entered the insurance industry in 1979 in the Claims and Engineering Department of a global insurance firm, where he became underwriting manager for its Oil and Petrochemical Division. He later worked for a Lloyd’s syndicate, where he became partner in charge of the Energy Division, including power and construction. He also worked for other major global underwriting firms, where he led their London and European underwriting energy and power operations. Additionally, he established an Energy Division, including both onshore and offshore property, power, and construction.

Mr. Gefers received his bachelor of arts degree in economics from Fordham University and bachelor of science degree in mechanical engineering from Polytechnic Institute of New York.

Alex J. Lathrop is a partner in Pillsbury Winthrop Shaw Pittman, LLP’s Litigation and Insurance Recovery and Advisory practices, located in Washington, DC, where he helps corporate policyholders recover from their insurers. 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—to obtain coverage under every major form of insurance.

Mr. Lathrop received his bachelor of arts degree from the University of California, Berkeley, and his juris doctorate from the University of Virginia School of Law. The 2005 and 2006 editions of Chambers USA, America’s Leading Lawyers for Business, recognized Mr. Lathrop as an “up and coming” insurance coverage attorney in Washington, DC.
Kyle Rogers
Risk Manager
HollyFrontier Corporation

Kyle Rogers serves as risk manager for HollyFrontier Corporation, an independent petroleum refiner in the United States with operations throughout the Mid-continent, Southwestern, and Rocky Mountain regions. Subsidiaries of HollyFrontier produce and market gasoline, diesel, jet fuel, asphalt, heavy products, and specialty lubricant products. Prior to joining HollyFrontier, Mr. Rogers was a senior analyst with Energy Future Holdings, a risk analyst with Oxy, and a claims examiner with Sedgwick CMS. He is active in the Risk and Insurance Management Society (RIMS), DFW Chapter, having served as president and currently serving as RIMS delegate.

Mr. Rogers received his bachelor of science degree from the University of North Texas and his master of business administration degree in management from the University of Dallas. He completed The Energy School at Saint Joseph's University. He also holds the Associate in Risk Management designation.
Hackers Are After More Than Just Data:  
Property Coverage for Physical Damage and 
Business Interruption Caused by a Cyber-Attack

Presented by:  
Kyle Rogers, Risk Manager,  
The HollyFrontier Companies  

Robert Gefers, Managing Director,  
Marsh | Energy & Power  

Alex Lathrop, Partner,  
Pillsbury Winthrop Shaw Pittman LLP  

#IRMI2017

What is Your Cyber Risk?

• “Cyber risk” is most often associated with privacy-related data breaches  
• Companies that maintain large amounts of customers’ personally  
  identifiable information, such as retail and health care companies, are  
  prime targets for hackers seeking to obtain or exploit personal information  
• Losses include costs to defend against class action lawsuits, investigation,  
  remediation and notification costs, crisis management, and identity  
  protection services  
• “Cyber insurance” is designed to cover these losses  
  • The market has grown as a form of E&O coverage  
  • Property Damage and Bodily Injury are excluded  
  • Business interruption limits are low in comparison to BI limits in property policies
What is Your Cyber Risk?

• Cyber attacks present a different type of risk for energy companies
• Hackers that target energy companies typically are not focused on personally identifiable information
  • They seek to damage and disrupt operations
• The types of losses that would result from a successful cyber attack on an energy company would be the same types of losses that would result from a natural disaster or industrial accident
  • Costs to repair and replace damaged equipment, extra expense, and loss of revenue until normal operations resume
• Unlike a natural disaster or industrial accident, losses from a cyber attack may not be limited to a particular geographic location or region

What “Cyber Insurance” Do You Have?

• What insurance is available to cover physical damage and business interruption resulting from a cyber attack?
  • Will traditional property policies respond?
    • Is cyber risk different than other perils?
    • Is a cyber attack a risk that your insurers intend to underwrite?
    • Is there a meeting of the minds between insurers and policyholders on these issues?
    • If your property policies contain cyber exclusions, how will those exclusions be applied?
    • Will ensuing loss be covered, even if the cyber attack is not?
What “Cyber Insurance” Do You Have?

• Insurers have begun to introduce “Cyber DIC” or “Cyber Wrap” policies
  • Designed to cover property damage, business interruption, and other losses resulting from cyber attacks but not covered by “traditional” P&C coverage
• Are these new insurance products the answer?
  • Are they redundant if you have “all risks” coverage?
  • Where do they fit in your program and when do they respond?

Cyber Attacks Causing Physical Damage – An Emerging Risk

• Publically reported instances of cyber-attacks on large industrial facilities causing physical damage and interrupted operations:
  • Sadara Chemical Company (a joint venture between the Saudi Arabian Oil Co. and Dow Chemical Co. operating a chemical complex in Jubail, Saudi Arabia, was forced to shut down its computer network after detecting the Shamoon virus) (January 2017)
  • Burlington Electric (malware potentially associated with Russian government hacking efforts found on employee laptop) (December 2016)
  • Ukraine Power Outage (hackers infiltrated two power distribution companies’ control systems and disconnected electrical substations) (2015)
Cyber Attacks Causing Physical Damage – An Emerging Risk

- Publicly reported instances of cyber-attacks on large industrial facilities causing physical damage and interrupted operations (cont.)
  - German Steel Mill (hackers infiltrated the industrial control system, causing blast furnace explosion resulting in “massive” damage) (2014)
  - Bowman Avenue Dam in Rye Brook, New York (after accessing the dam’s industrial control system, hacker gained control of a computer that opened and closed the dam’s sluice gates) (2013)
  - Stuxnet (computer worm used to sabotage centrifuges in Iran’s Natanz nuclear facility) (2010)
  - Oil Pipeline in Turkey (hackers accessed the industrial control system and super-pressurized the crude oil until the pipeline exploded) (2008)

Cyber Attacks Causing Physical Damage – An Emerging Risk

- Cyber attacks on energy, utility, and large manufacturing companies are reportedly taking place with increasing regularity
  - Department of Energy’s Quadrennial Energy Review (January 2017)
    - “attacks elsewhere in the world on energy systems should be seen as an indicator of what is possible”
  - HM Government and Marsh report on UK Cyber Security, the Role of Insurance in Managing and Mitigating the Risk
Will Your Insurance Be There When You Need It?

• Coverage for a company’s losses resulting from a cyber attack will depend on the facts of the loss and the language of the particular policies involved

• In general, insurers have acknowledged that physical damage and business interruption caused by a cyber-attack may be covered under traditional property policies
  • Some underwriters contend this is not their intent, even under all risk policies
  • In contrast, FM Global has taken position that a data breach is physical damage, and FM Global policies cover resulting loss, subject to other terms and conditions of the policies
    • Beware of sub-limits

• There does not appear to be a unified view within the insurance industry

Will Your Insurance Be There When You Need It?

• Some industry publications have acknowledged that policyholders reasonably expect coverage for cyber losses under traditional policies

• “A.M. Best’s View on Cyber-Security Issues and Insurance Companies,” Best’s Special Report (Nov. 24, 2015)
  • Acknowledges that “data breaches [causing] physical damage . . . are currently covered under traditional insurance products such as Commercial General Liability Policies (CGLP), Business Interruption (BI), or Directors & Officers (D&O)[,]” and that “Policyholders may expect coverage under CGLP/BI/D&O for cyber-attacks . . . given the general language in such policies . . . .”
Will Your Insurance Be There When You Need It?

• Some insurers suggest there is a “mismatch of expectation” between insurers and policyholders regarding coverage
  • Notably, these insurers acknowledge that physical damage and business interruption losses from cyber attacks may fall within the policy language
    • Acknowledges that all risks property policies “are commonly silent on whether cyber-related losses would be paid” and that “purchasers of insurance may think they are protected against losses from cyber, where insurers think that these customers have not purchased cover for it. . . . This mismatch of expectation and reality could be expected to generate disputes in the event of a large scale cyber loss.”

Will Your Insurance Be There When You Need It?

• Some exclusions have been introduced specifically addressing cyber attacks
  • Institute Cyber Attack Exclusion Clause (CL 380)
    “[I]n no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to, by, or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.”
  • Terrorism Form (LMSA 3030)
    “This Policy does not insure against . . . Loss or damage by electronic means including but not limited to computer hacking or the introduction of any form of computer virus or corrupting or unauthorised instructions or code or the use of any electromagnetic weapon.”
Will Your Insurance Be There When You Need It?

• Whether and how cyber exclusions apply will depend on several factors
• Principles of insurance policy interpretation limit the application of exclusions
  • The insurer bears the burden of showing that an exclusion applies
  • Exclusions must be (1) narrowly construed, (2) clearly and unmistakably stated, and (3) subject to no other reasonable interpretation
• The insurer must demonstrate that the exclusion applies to the facts of the particular loss
  • For example, for CL380 to apply, the computer, computer system, computer software program, malicious code, computer virus or process or other electronic system must be used or operated “as a means for inflicting harm.”
  • How will the insurer demonstrate the hacker’s intent?

How Traditional Property Policies May Apply to Cyber Attacks

• Scenario 1: A cyber-attack interrupts an energy company’s operations, without harm to the plant’s equipment, resulting in business interruption losses
  • The cyber-attack is carried out by a virus that causes the industrial control system to malfunction, requiring all operations to be shut down for an extended period of time

• Coverage issues:
  • Can the forced shutdown of a company’s operations constitute “direct physical loss” or “direct physical damage?”
    • Property policies typically require “direct physical loss of or physical damage to Property Insured” to trigger business interruption coverage
  • Does manipulation or destruction of data constitute “direct physical loss?”
How Traditional Property Policies May Apply to Cyber Attacks

- **Scenario 2:** A cyber-attack causes a plant explosion, damaging equipment and resulting in an extended shutdown

- **Coverage issues:**
  - Is the cyber attack itself or the resulting explosion a covered peril?
    - Under an all risks policy
    - Under a Named Peril policy
  - If the loss results from a covered peril, do any exclusions or limitations apply?
  - If the cyber attack is not a covered peril, is the ensuing loss covered?
  - If the cyber attack falls within an exclusion, is the ensuing loss covered?

New Insurance Products for Cyber Losses

- Insurers have begun to introduce new cyber policy forms that are marketed as filling gaps in a policyholder’s existing P&C program

- **Examples include:**
  - DIC coverage or “cyber wrap” coverage
    - Coverage for cyber attacks that sits above property tower and/or other coverages and applies as differences-in-condition coverage
  - Pure business interruption coverage
    - No “physical damage” requirement