Hackers Are After More Than Just Data: Will Your Company's Property Policies Respond When Cyber Attacks Cause Physical Damage and Shut Down Operations?

Alex J. Lathrop* and Janine M. Stanisz*

Recent attention on high profile data breaches has overshadowed a potentially greater risk: cyber attacks on large industrial companies causing physical damage, potentially releasing contaminants, and shutting down operations. A handful of publicly reported cyber-attacks, including explosions at an oil pipeline and a steel mill, have highlighted the potential vulnerability of these companies' internet-facing industrial control systems to hackers. The insurance industry has reacted to the growing risk of privacy-related data breaches by marketing and selling so-called "cyber policies." But these policies typically exclude coverage for property damage and are ill-suited to cover the magnitude of business interruption losses that could result from an extended shutdown of a large industrial operation. That leaves policyholders to look to their traditional property policies. This article examines the cyber-attack risk that large industrial companies face and how those companies' traditional property insurance policies may help mitigate that risk.

---

* Alex J. Lathrop is a partner in Pillsbury Winthrop Shaw Pittman LLP's Litigation and Insurance Recovery and Advisory practices, 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. He has particular expertise in recovery for environmental losses.

* Janine M. Stanisz is an associate in Pillsbury Winthrop Shaw Pittman LLP's Litigation and Insurance Recovery & Advisory practices. Ms. Stanisz is a commercial litigator who concentrates her practice in advising and representing individual and corporate policyholders in coverage disputes involving first-party property damage/business interruption, product recall and professional liability policies.

This is an Accepted Manuscript of an article that was published on June 22, 2016, on Taylor & Francis Online and is available at: http://www.tandfonline.com/doi/full/10.1080/10406026.2016.1197653

Unauthorized attempts to access a business's computer systems and networks, commonly referred to as a "cyber attack," have become commonplace. The most commonly discussed risk associated with these attacks is a data breach, typically defined as a security incident that results in disclosure of private information to an unauthorized third party. Highly publicized data breaches affecting retail companies, such as Target and Home Depot, and various healthcare providers, have illustrated the potential costs and reputational harm that can result from these attacks. And while these high profile breaches are larger than most, they otherwise are not anomalies – smaller scale breaches are reported almost daily and are only increasing in frequency. Verizon's 2016 Data Breach Investigations Report identified 2,260 data breaches in 2015, up from 2,122 in 2014.[1] 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 the Ponemon Institute's 2015 Costs of Data Breach Study, the average total cost to a U.S. company of a data breach in 2014 was $6.5 million.[2]

As the risk of data breaches has grown, so has the market for so-called "cyber policies," a specialized form of insurance designed to cover some of the costs arising out of a data breach. But while cyber policies are an important part of a company's strategy for managing cyber risk, they are not a panacea. As the CEO of one of the largest players in the cyber insurance market has confirmed, cyber insurance capacity is very small compared to coverage companies buy for other property and casualty risks.[3] According to an industry survey, in 2015 cyber insurance was purchased by only 30% of companies with revenues over $300 million; for companies with revenues over $5 billion, the number only increased to 35%.[4] Moreover, the cyber insurance limits purchased by these companies are relatively small in comparison to the property and casualty limits they typically buy. For example, according to the same industry survey, companies with revenues between $300 million and $1 billion bought on average $7.5 million in cyber insurance limits in 2015, while the majority of comparably sized companies bought over $40 million in property limits (and many bought over $100 million).[5] The difference becomes starker as the size of a company increases: companies with revenues over $5 billion bought on average $34 million in cyber insurance limits compared to over $500 million in property limits.[6]

---

1 Verizon, 2016 Data Breach Investigations Report at 9, *available at* http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

2 Ponemon Institute, 2015 Costs of Data Breach Study: United States (May 2015) at 1, *available at* https://www-01.ibm.com/marketing/iwm/dre/signup?source=ibm-WW_Security_Services&S_PKG=ov34982&S_TACT=000000NJ&S_OFF_CD=10000253&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=70726441271914635145472&cm_mc_sid_50200000=1463525547.

3 Rachael King, Cyber Insurance Capacity is 'Very Small': AIG CEO, The Wall Street Journal (April 2, 2015).

4 2016 RIMS Benchmark Survey at 14 (New York, Advisen Ltd., 2016).

5 *Id*. at 14, 119.

6 *Id*. It is important to note that these numbers are only averages, and only reflect the data provided in response to the referenced survey. Many companies buy substantially more cyber insurance limits than the average amounts referred to above, and many companies may be unwilling to disclose the amount of insurance they buy. Moreover, there are a number of new cyber insurance products currently being offered, including so-called "difference in conditions" policies, which may provide substantially more limits than more traditional cyber policies.

As these numbers illustrate, privacy-related data breaches represent a substantial risk in the aggregate. And they represent a significant – albeit not catastrophic – risk to individual companies, which can be mitigated to some degree by the purchase of specialized insurance.

This article addresses a different type of cyber risk that, for the most part, goes beyond the coverage provided by cyber polices – the risk of physical damage and related business interruption caused by a cyber attack. Although less publicized than privacy-related data breaches, there have been a handful of instances in which cyber attacks have targeted the process control systems of large industrial companies for the purpose of causing a malfunction, resulting in property damage and a disruption of the company's operations. Due to the nature of the operations of these large industrial companies, the property damage is likely to include environmental pollution. While these cyber 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. Moreover, cyber insurance policies ordinarily contain an exclusion for loss resulting from or arising out of property damage (and bodily injury), typically defined as physical injury to or destruction of any tangible property, including any loss of use of tangible property. And while cyber policies often do 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 purchased.

Against this backdrop, this article examines whether physical damage and business interruption losses caused by a cyber attack may be covered under a company's traditional property policies. First, we describe in greater detail the nature of the risk from cyber attacks that energy, infrastructure, and other large industrial companies currently face. Second, we discuss a surprisingly candid acknowledgement within the insurance industry that many traditional property policies are "silent" regarding whether losses caused by a cyber attack are covered – i.e., coverage for such losses is not expressly excluded, notwithstanding that the insurers are well aware that the risk exists. Finally, we describe three hypothetical cyber attacks, each resulting in a different type of loss, and discuss whether traditional property policies might provide coverage. As is always the case in questions of insurance coverage, the answer ultimately turns on the language of the particular policies the company purchased. But as a general matter, 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.

I. THE NATURE OF THE RISK

Companies that operate large, complex industrial processes, such as energy, oil and gas, mining, chemical, transportation, and manufacturing companies, use centralized computer systems, referred to generically as industrial control systems ("ICS"), to constantly monitor, collect data from, supervise, and control remote, geographically dispersed units. "These control systems are critical to the operation of the U.S. critical infrastructures that are often highly interconnected

and mutually dependent systems."[7] Given their interconnected nature, these systems are vulnerable to unauthorized access by hackers through the internet.[8] Not surprisingly, companies in these industries have become targets for cyber-attacks. However, unlike hackers targeting retail and healthcare companies, among others, hackers targeting these companies typically are after more than just data. "Operational sabotage" reportedly is the greatest information technology security threat such companies face.[9]

Data from several sources confirm that cyber attacks on companies' industrial control systems are taking place with increasing regularity.

- The Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"), which is part of the U.S. Department of Homeland Security, responded to 198 reported cyber incidents in 2012 across all critical infrastructure sections.[10] 41% of these reported incidents targeted companies in the energy sector, particularly electricity.[11] By 2014, the number of cyber attacks reported and responded to by ICS-CERT rose to 245, of which 32% targeted energy companies, and 27% targeted critical manufacturing companies.[12]

- A report on cyber security published by the UK Trade & Investment department of the UK Government found that "[p]hysical losses are a growing concern – both in term of severity and frequency . . . ."[13] Discussing industrial control systems in the energy sector is an example of this "new category of risk," the report observed that "these new generation control systems are built on the concept of openness

---

7 Keith Stouffer, Joe Falco, Karen Scarfone, Guide to Industrial Control Systems (ICS) Security, Recommendations of the National Institute of Standards and Technology at 2-1, National Institute of Standards and Technology, Special Publication 800-82 (June 2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

8 *See* Trend Micro & Organization of American States, Report on Cybersecurity and Critical Infrastructure in the Americas (2015), *available at* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf, at p. 1 ("[A]s countries of the Americas have experienced a growth in the number of infrastructures running on Internet-facing networks, so the number of cyber-attacks to the same infrastructures has increased, which could compromise a country's critical infrastructure and ability to provide essential services to its citizens.").

9 UPI, Cyber and Network Security a Threat to Energy Companies (May 31, 2013), *available at* http://www.upi.com/Business_News/Energy-Industry/2013/05/31/Cyber-and-network-security-a-threat-to-energy-companies/58271370022982/.

10 Bipartisan Policy Center, Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat (Feb. 2014), *available at* http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Cybersecurity%20Electric%20Grid%20BPC.pdf, at p. 17.

11 *Id.*

12 ICS-CERT Monitor, Incident Response/Vulnerability Coordination in 2014 (Sept. 2014 - Feb. 2015), *available at* https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf.

13 HM Government and Marsh, UK Cyber Security, the Role of Insurance in Managing and Mitigating the Risk (Mar. 2015), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf, at 13.

and interoperability, and this has exposed the sector to a host of cyber security risks that are only just beginning to be understood."[14]

- According to a joint report by The Aspen Institute and Intel Security that polled experienced technology and security professionals from 625 critical infrastructure organizations regarding cyber attacks on their companies: "Almost nine out of 10 have experienced at least one attack on secure systems in their organization over the past year, with a median of close to 20 attacks per year. More than 59% of confirmed cyberattacks resulted in physical damage, more than 33% resulted in service interruption, and more than 25% resulted in data compromise . . . ."[15] The report also noted:

  > Almost half the security professionals surveyed think it is likely or extremely likely that a successful cyberattack will take down critical infrastructure and cause loss of human life within the next three years.[16]

- In response to a survey of critical infrastructure companies sponsored by The Organization of American States, 76% of respondents stated that cyber-attacks targeting infrastructure were getting more sophisticated, and 54% of respondents' organizations experienced attempts to manipulate their organization's equipment through a control network/system.[17]

A recent Wall Street Journal article reported on a specific example of the type of attack referred to in these various reports. The article described how a hacker was able to gain access to a computer system that controlled the Bowman Avenue Dam in Rye Brook, New York, using a process known as "Google dorking."[18] This method allows hackers to identify and obtain access to unprotected computers through websites connected to U.S. infrastructure by using a variety of technical search terms designed to find security holes in the configuration and computer code that websites use.[19] Once the hacker accessed a Bowman Avenue Dam computer, he used more sophisticated techniques to hack into the dam's industrial control system, ultimately accessing a computer that controlled the dam's sluice gates.[20] Ultimately, 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. However, the ability of the

---

[14] *Id*.

[15] The Aspen Institute & Intel Security, Critical Infrastructure Readiness Report (2015), *available at* http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf, at p. 5.

[16] *Id.* at 6.

[17] Trend Micro & Organization of American States, Report on Cybersecurity and Critical Infrastructure in the Americas (2015), *available at* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/critical-infrastructures-west-hemisphere.pdf, at pp. 2, 50.

[18] Christopher M. Matthews, Google Search Technique Aided N.Y. Dam Hacker in Iran, The Wall Street Journal (Mar. 27, 2016), *available at* http://www.wsj.com/articles/google-search-technique-aided-n-y-dam-hacker-in-iran-1459122543.

[19] Hilary Brueck, 'Dorky' Google Search Helped Hacker Bust into a New York Dam, Fortune (Mar. 28, 2016), *available at* http://fortune.com/2016/03/28/dorky-google-search-helped-hacker-bust-into-a-new-york-dam/

[20] *Id*.

hacker to access the dam's industrial control system demonstrates a "frightening new frontier for cybercrime," as it was made possible because "computers controlling industrial and infrastructure systems are old and predate the consumer Internet."[21]

II. PUBLICALLY REPORTED INSTANCES OF CYBER-ATTACKS CAUSING PHYSICAL DAMAGE

There have been at least four publically reported cyber-attacks on large industrial facilities that caused physical damage and interrupted operations, each of which is described briefly below.

- Turkey Oil Pipeline. In 2008, hackers accessed the industrial control system of a Turkish oil pipline 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. They were able to gain access to the control system through the surveillance cameras. Once inside, the hackers located a computer running on a Windows operating system that was in charge of the alarm-management network and shut down the alarm system so that the increased pressure in the pipeline would go undetected. [22]

- Stuxnet. In 2010, a computer worm known as Stuxnet, which spread via infected USB drives, was used to sabotage centrifuges in Iran's Natanz nuclear facility. The centrifuges were used to enrich uranium for use in nuclear weapons. 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.[23]

- German Steel Mill. Using a method known as "spear phishing," (sending targeted emails that appear to come from a trusted source that direct the recipient to inadvertently allow malware to be downloaded), hackers infiltrated the control system of a steel mill. They then caused numerous individual components and systems to fail such that a blast furnace could not be properly shutdown, resulting in "massive" damage.[24]

- Ukraine Power Outage. In 2015, over 80,000 people in Ukraine lost power when hackers infiltrated two power distribution companies' control systems and

---

[21] Christopher M. Matthews, Google Search Technique Aided N.Y. Dam Hacker in Iran, The Wall Street Journal (Mar. 27, 2016), *available at* http://www.wsj.com/articles/google-search-technique-aided-n-y-dam-hacker-in-iran-1459122543 (quoting U.S. Attorney Preet Bharara).

[22] Jordan Robertson & Michael Riley, Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar (Dec. 10, 2014), *available at* http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

[23] InsuranceLinked, Weaponising the internet – the rise of physical cyber attacks, *available at* http://insurancelinked.com/weaponising-the-internet-the-rise-of-physical-cyber-crime/ (Aug. 3, 2015).

[24] Kim Zetter, Cyberattack has Caused Confirmed Physical Damage for the Second Time Ever, WIRED (Jan. 8, 2015), *available at* http://www.wired.com/2015/01/german-steel-mill-hack-destruction/.

> disconnected electrical substations. To further exacerbate the problem, hackers also attacked the utility company's service helpline, preventing customers from reporting the outage.[25]

It is not difficult to imagine the wide ranging losses that could result from the sorts of cyber attacks described above. As the Turkish pipeline explosion illustrates, a cyber attack can cause an oil or chemical spill that can contaminate the company's property, as well as third-party property. A plant explosion such as the one that took place at the German Steel Mill can cause massive damage to the plant itself, and a power outage can result in wide-ranging damage to companies with operations that rely on electricity. And, of course, all of these events can result in substantial losses of revenue while operations are interrupted. As the UK Trade & Investment cyber security report noted, companies that experience cyber attacks are faced with direct physical damage, business disruption, data/software deletion, direct financial loss, damage to intellectual property, third-party liabilities, reputational loss, and investigation and response costs.[26] Among these losses, "[p]hysical losses are a growing concern – both in terms of severity and frequency . . . ."[27]

III. INSURERS HAVE ACKNOWLEDGED THAT PHYSICAL DAMAGE AND BUSINESS INTERRUPTION CAUSED BY A CYBER-ATTACKS PRESENT A SIGNIFICANT RISK OF LOSS THAT MAY BE COVERED UNDER TRADITIONAL PROPERTY POLICIES

The insurance industry has recognized that cyber-attackers may cause physical damage and business interruption, and that such losses may in fact be covered under traditional insurance products, including property and commercial general liability policies. A report on cyber-security issues facing insurers from A.M. Best, which provides credit ratings and financial data for insurance companies, 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 . . . ."[28] Suggesting that the policyholders' expectation of coverage may be unfounded, as these traditional insurance products were "developed decades ago at a time when cyber liability claims were not contemplated[,]" the A.M. Best Report suggests that insurers can avoid "long and expensive litigation" by "designing, developing, and selling specifically targeted types of specialty coverage forms addressing cyber liability risks

---

[25] Kim Zetter, Everything We Know About Ukraine's Power Plant Hack, WIRED (Jan. 20, 2016), *available at* http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.; Dan Goodin, First Known Hacker caused power outage signals troubling escalation, Ars Technica (Jan. 4, 2016), *available at* http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/.

[26] HM Government and Marsh, UK Cyber Security, the Role of Insurance in Managing and Mitigating the Risk (Mar. 2015), *available at* https://www.gov.uk/government/uploads/system/uploads/ ttachment_data/file/415354/ UK_Cyber_Security_Report_Final.pdf, at p. 8.

[27] *Id.* at 13.

[28] A.M. Best's View on Cyber-Security Issues and Insurance Companies, Best's Special Report (Nov. 24, 2015), *available at* http://www.bestweek.com/europe/promo/AMBViewCyberSecurity.pdf, at p. 1, 4.

separate from CGLP/BI/D&O."[29] To be sure, the development of specialized coverage may support an argument that data breaches typically such be covered under cyber policies rather than general liability policies, it also *supports* the conclusion that cyber-related physical damage and related business interruption losses still fall within traditional property polices. After all, as discussed above, the specialty cyber policies developed to date exclude losses arising out of property damage. Moreover, the argument that broadly worded policies should not be interpreted to cover a type of claim that "was not contemplated" at the time the language was drafted is a familiar one. It is, for example, the same argument insurers have made when attempting to avoid coverage for environmental claims under historical occurrence-based comprehensive general liability policies. With respect to current property and business interruption policies, this argument does not take into account the fact that the policies are sold on an annual basis, at which time the insurers have the ability to include clear language excluding coverage for cyber-related losses.

Another rather striking acknowledgment of potential coverage for physical damage and business interruption losses caused by cyber attacks appears in a 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 US Power Grid" (the "Lloyd's Report").[30] The Lloyd's Report considers "the broad range of claims that could be triggered by disruption to the US power grid" resulting from a hypothetical cyber attack causing an estimated $243 billion in economic loss, with total claims paid by the insurance industry estimated between $21.4 billion and $71.1 billion.[31] The Lloyd's Report draws a distinction between what it terms an Information Technology (IT) attack, "such as a data breach," and an Operational Technology (OT) attack, "such as an attack on a manufacturing plant," and acknowledges that an OT attack "may activate both first and third party business interruption policies as well as property damage policies if physical damage occurs."[32] Echoing the A.M. Best report, The Lloyd's Report suggests that coverage for these OT attacks under traditional "all risks" property policies may not be intended:

> Insurers are also realising that the cyber threat has the potential to generate claims from lines of insured business where cyber damage is not an explicit cover. This 'silent' cyber exposure refers to instances where claims may arise under an all risks cover. Insurers may not realise the extent of their exposure to this emerging threat class, and may not have charged premium to cover this aspect of the risk. Insurers may be holding more cyber exposure in unexpected lines of business in their portfolio than they realise.[33]

---

[29] *Id*.

[30] Lloyd's & Centre for Risk Studies, Business Blackout, The Insurance Implications of a Cyber Attack on the US Power Grid (2015), *available at* https://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf.

[31] *Id*. at 4-5.

[32] *Id*. at 25.

[33] *Id.*

Given the significant amount of attention cyber risk has received by the media, government agencies, brokers, and policyholders, it is perhaps disingenuous to suggest that insurers are unaware of the cyber exposure they face under traditional lines of coverage. As insurers agree to renew their policyholder's property and business interruption coverage programs year after year 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. Tellingly, in estimating the loss to the insurance industry, the Lloyd's Report assumes that claims made by power generation companies under their property policies for damaged power generators and resulting business interruption loss would be covered.[34]

Although acknowledging the potential for coverage under traditional lines of coverage, the Lloyd's Report estimates that insurers would only make claims payments totaling $21.4 billion out of an estimated $243 billion in total damage. Thus, there is a clear gap in coverage in this hypothetical scenario. However, the assumption by Lloyd's that nearly $222 billion in damages would be uninsured is in tension with its acknowledgment that traditional insurance programs are silent on whether such losses would be covered:

> Property covers and 'all risks' descriptions are commonly silent on whether cyber-related losses would be paid. Insurers may assume that their exclusion language and conventional interpretation of coverages will protect them from future claims from cyber events, while purchases 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.[35]

As the Lloyd's Report acknowledges, "[i]f the insurers are silent on the issue, then it is open to interpretation whether or not the general policy covers certain cyber events."[36]

The admissions 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 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 be compromised by the parties or decided by the courts. The role of a court in interpreting an insurance policy in the first instance 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 losses, this leads to only two alternatives: (1) the clear language of the policies is broad enough to encompass losses resulting from cyber attacks even if there is no express coverage for such losses, or (2) the policies are subject to more than one reasonable interpretation, and therefore are ambiguous. Under the general principles of

---

[34] *Id*. at 29-30.

[35] *Id*. at 37.

[36] *Id.* at 25.

insurance interpretation, ambiguities are resolved in the insured's favor and in line with the insured's reasonable expectations.[37] Thus, under either alternative, 'all risks' policies that are silent with respect to coverage for cyber-related losses should be interpreted to cover them.

Indeed, the Lloyd's Report expressly identifies "a number of areas where there could be significant ambiguity around how coverage will be interpreted and whether claims could reasonably be expected to be successful or denied."[38] These include "ambiguity around the peril definition" and whether cyber-attacks that impact multiple industrial units (power generators, in the case of the hypothetical power outage) would constitute a single event or multiple events for the purpose of determining the number of applicable deductibles or retentions.[39]

Finally, the Lloyd's Report observes that insurers are developing new exclusions specifically designed to limit coverage for cyber events in part because the present exclusions do not currently address the implications of cyber-attacks. For example, Exclusion Institute Cyber Attack Exclusion Clause (CL 380), and Terrorism Form (LMSA 3030), have been designed to bar coverage for claims relating to cyber-attacks that are committed with malicious intent or are deemed acts of war. Additionally, the Exclusion Information Technology Hazards Clarification clause, Electronic Data Endorsement A, and Electronic Data Endorsement B,[40] are designed to bar coverage for property damage claims that may result from cyber-attacks, unless the resulting property damage is caused by a fire or explosion. Importantly, 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.[41] Moreover, the creation of new exclusions specifically designed to apply to losses due to cyber attacks supports that exclusions contained in policy forms that were drafted many years ago were not intended to apply to cyber related losses.

IV. HOW TRADITIONAL PROPERTY POLICIES MAY APPLY TO DAMAGE CAUSED BY CYBER-ATTACKS

Whether property damage or business interruption losses caused by a cyber attack will be covered under a company's traditional property policy ultimately will depend on the specific language of the particular policy or policies purchased by the company. While standard form property policies exist, the larger a company is, the less likely it is to purchase such standard form coverage. Rather, the language in property policies purchased by large industrial companies, such as those in the energy, oil and gas, mining, chemical, transportation, and manufacturing industries, often will vary depending upon the industry, broker, insurer, length of

---

37 *See e.g. Voorhees v. Preferred Mut. Ins. Co.*, 607 A.2d 1255, 1260 (N.J. 1992) (citations omitted).

38 Lloyd's Report, at 37.

39 *Id*.

40 *Id*. at 38.

41 *Continental Cas. Co. v. Rapid-American Corp.*, 593 N.Y.S.2d 966, 971 (N.Y. 1993); *Hartford Accident & Indem. Co. v. Wesolowski*, 350 N.Y.S.2d 895, 898 (N.Y. 1973); *Colonial Tanning Corp. v. Home Indem. Co.,* 780 F. Supp. 906 (N.D.N.Y. 1991); *Savoy Med. Supply Co. v. F & H Mfg. Corp.*, 776 F. Supp. 703 (E.D.N.Y. 1991).

the company's relationship with the underwriter, and numerous other factors. These companies do not buy "off the shelf" form policies, but instead buy so-called "manuscript policies." Manuscript policies still are drafted by insurers, but they typically include language that the 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. Against the backdrop, below we discuss how traditional property policies may apply to cover cyber-related losses in three hypothetical scenarios.

- **Hypothetical #1: A cyber-attack interrupts a manufacturing company's operations, without harm to the plant's equipment, resulting in business interruption losses**

  The policyholder is a large manufacturing company that uses a centralized industrial control system to run operations at numerous geographically dispersed units. A hacker accesses the system through the internet and causes a number of internal system malfunctions in remote units that trigger an automatic shutdown of the entire manufacturing process. Further, the hacker installs malware containing malicious code that causes the industrial control system to continue to incorrectly detect errors in remote units even after the units have been fixed such that it will not allow the manufacturing process to come back on line. There is no physical destruction of the manufacturing equipment or the goods being manufactured; there is no fire or explosion, or spoilage. Other than the cost of hiring vendors to investigate and remediate the cyber attack, the only loss suffered by the company is lost revenue due to interruption of its operations. The amount of the loss is substantial and the shutdown continues well beyond the waiting period required under the business interruption coverage.

A typical property policy provides coverage for "*direct physical loss of or direct physical damage to* the Property Insured, provided that such loss or damage results from an Occurrence that first commences during the Period of Insurance . . . ." Additionally, a policy's business interruption coverage ordinarily is tied to "physical loss of or physical damage to Property Insured." Thus, the in order to trigger the business interruption coverage, there must first be *"direct physical loss of or direct physical damage."*

A. Shut Down of the Manufacturing Process Itself May Constitutes "Direct Physical Loss" or "Direct Physical Damage"

Many courts have held that "direct physical loss or damage" does not require tangible, structural damage to insured property that is permanent, but instead includes events where property is rendered unusable or its function impaired. For example, in *Wakefern Food Corp. v. Liberty Mutual Fire Insurance Co.*, the New Jersey Appellate Division considered a case where physical

damage was temporary and non-structural.[42] The policyholders, a group of supermarkets, purchased "all-risks" property insurance from Liberty Mutual, including a "Services Away From Covered Location Coverage Extension," which extended coverage for consequential loss or damage resulting from an interruption of the electrical power to plaintiffs' supermarkets. In August 2003, the North American power system experienced problems that resulted in a four-day electrical blackout in large portions of the Midwest and Northeast United States and Ontario, Canada. The policyholders suffered losses relating to food spoilage and loss of business and submitted an insurance claim. Liberty Mutual denied coverage and asserted that plaintiffs were unable to present any evidence that the "transmission lines, connections or supply pipes which furnish electricity" had been physically damaged.

The Court disagreed and determined that the electrical grid "was 'physically damaged' because, due to a physical incident or series of incidents, the grid and its component generators and transmission lines were physically incapable of performing their essential function of providing electricity."[43] While some evidence was proffered demonstrating that certain generators may have incurred physical damage, the Court found damage to specific equipment unnecessary. Rather, the Court held that the grid was physically damaged because "the entire system was incapable of producing power for several days."[44] Under this analysis, a cyber-attack that causes a manufacturing plant to be rendered inoperable, without specific damage to equipment, could nevertheless meat the "directly physical loss or damage" requirement sufficient to trigger business interruption coverage.

Similarly, a number of other courts have reasoned that "*direct physical loss of or direct physical damage*" occurs where property can no longer be used for its intended purpose. *See E.g.*, *Western Fire Ins. Co. v. First Presbyterian Church*, 165 Colo. 34, 36-39 (1968) (infiltration of gasoline in soil under and around church which led to vapors contaminating the church and rendering it uninhabitable was a "direct physical loss"); *Port Authority of New York and New Jersey v. Affiliated FM Ins. Co.*, 311 F.3d 226, 236 (3d Cir. 2002) (presence of large quantities of asbestos in the air of a building that renders the building unusable is "physical loss or damage"); *Gregory Packaging, Inc. v. Travelers Prop. Cas. Co. of Am.*, 2014 WL 6675934, at *5-7 (D.N.J. Nov. 25, 2014) (release of ammonia in facility that rendered facility unfit for occupancy was "direct physical loss of or damage to" the facility). Still, other courts have commented that "direct physical loss" provisions "require only that a covered property be injured, not destroyed." *Sentinel Mgmt. Co. v. N.H. Ins. Co.*, 563 N.W.2d 296, 300.

B. The Manipulation or Destruction of Data May Constitute "Direct Physical Loss"

The cyber hack itself also may constitute direct physical loss or damage. In the hypothetical, the hacker caused a number of internal system malfunctions in remote units that triggered the automatic shutdown of the manufacturing process, and the hacker installed malware containing

---

[42] 406 N.J. Super. 524, certif. denied 200 N.J. 209 (2009).

[43] *Id.* at 734.

[44] *Id.* at 544.

malicious code that caused the industrial control system to malfunction. Some courts have found that the corruption of electronic data constitutes direct physical loss or damage.

As one Louisiana federal court observed, "[t]he question of whether electronic data is physical or non-physical has been debated in several jurisdictions and has led to various conclusions."[45] In *Lambrect & Associates, Inc. v. State Farm Lloyds*,[46] a computer server, pre-packaged software and data stored on the server was destroyed by a virus, requiring that each be replaced.[47] The insurer, State Farm, asserted that coverage was barred because electronic media and records and the data stored on them was not physical. The court disagreed and held that the destruction of the server, software and data constituted "direct physical loss." The policy stated that "State Farm 'will not pay for any loss of 'business income' caused by accidental direct physical loss to 'electronic media and records'" until after a designated time period passed. The court held that:

> In the section of the policy defining coverage for loss of income, "electronic media and records" is defined as a. electronic data processing, recording or storage media such as films, tapes, discs, drums or cells; b. data stored on such media; or c. programming records used for electronic data processing or electronically controlled equipment.
>
> We hold that the plain language of the policy dictates that the personal property losses alleged by [the insured] were "physical" as a matter of law. . . . [T]he server falls within the definition of "electronic media and records" because it contains a hard drive or "disc" which could no longer be used for "electronic data processing, recording, or storage." The data that [the insured] lost as a result of data is also covered because it was the "data stored on such media."[48]

The United States Court of Appeals for the Fourth Circuit also found that destruction of data alone constitutes property damage. In *NMS Services, Inc. v. The Hartford*, a software development company's system was hacked, resulting in the destruction of computer files and databases.[49] The Court held that NMS was entitled to business income coverage. The provision provided that Hartford would "pay for the actual loss of Business Income [to NMS] sustain[ed] due to the necessary suspension of [NMS's] 'operations' during the 'period of restoration.' The suspension *must be caused by direct physical loss of or damage* to property at the described premises."[50] The Court held that NMS suffered damage to its computers when its files were destroyed. Accordingly, even if a hacker destroys only data and no other tangible property, arguably the destruction of data constitutes direct physical loss or damage that triggers coverage for lost income (i.e., business interruption).

---

[45] *Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs, Inc.*, No. 10-809 Section B, 2012 U.S. Dist. LEXIS 45184 at * 8 (Mar. 30, 2012).

[46] 119 S.W.3d 16 (Tex. Ct. App. 2003).

[47] *Id.* at 25.

[48] *Id.* at 25

[49] 62 Fed. Appx. 511 (4th Cir. 2003).

[50] *Id.* at 514 (emphasis added).

However, some courts have reached a different result. In *Ward Gen. Ins. Servs, Inc. v. The Employers Fire Ins. Co.*,[51] the insured sought coverage for costs it incurred in recovering data and business loss after its data was inadvertently deleted during a computer system upgrade. The policy required a physical loss to trigger coverage. The Court held that the loss was not physical:

> (1) We fail to see how *information*, *qua* information, can be said to have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch. To be sure, information is stored in a physical medium, such as a magnetic disc or tape, or even as papers in three-ring binders or a file cabinet, but the information itself remains intangible. Here, the loss suffered by plaintiff was a loss of information, i.e., the *sequence* of ones and zeroes stored by aligning small domains of magnetic material on the computer's hard drive in a machine readable manner. Plaintiff did not lose the tangible material of the storage medium. Rather, plaintiff lost the stored *information*. The sequence of ones and zeros can be altered, rearranged, or erased, without losing or damaging the tangible material of the storage medium.
>
> (2) We conclude the loss of the database, with its consequent economic loss, but with no loss of or damage to tangible property, was not a "direct physical loss of or damage to" covered property under the terms of the subject insurance policy, and, therefore, the loss is not covered. Although counsel have cited no California cases addressing this issue, nor have we found any, our conclusion is consistent with cases decided on closely related issues.[52]

Given that insurance coverage disputes are governed by state law, the jurisdiction in which the dispute is heard (or the state's law that is applied) can have a profound impact on the coverage analysis for cyber-attacks.

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

  The policyholder is a petrochemical company operating a large refinery with numerous related processes, all controlled by an industrial control system. A hacker accesses the industrial control system and sets off a series of malfunctions at the crude oil distillation unit, the initial unit in the refining process that separates the crude oil into streams for further processing, causing the unit to explode. The explosion destroys the crude oil distillation unit and severely damages a number of nearby units. Because the crude oil distillation unit is the first step in the refining process, the entire refinery is shut down for an extended period of time.

---

[51] 114 Cal. App. 4th 548 (2003).

[52] *Id.* at 556-57.

Whether the damage to the refinery and resulting business interruption loss is covered will turn on whether the damage was caused by a covered peril and, if so, whether any exclusions in the policy apply.

A. Either the Cyber Attack or the Resulting Explosion May Be a Covered Peril

Generally, there are two types of property policies – "named peril" and "all risk." Under a named peril policy, coverage is available only for damage caused by perils specifically listed in the policy, such as fire, explosion, lightening, windstorm, theft, vandalism, etc. Cyber-attacks are unlikely to be among the listed perils and therefore coverage under a named peril policy would depend on whether the cyber-attack falls within the definition of a one of the named perils (such as vandalism). Alternatively, while the cyber attack may not fall within a named peril, the resulting explosion may, in which case the argument would be that the explosion was the proximate cause of the damage. All risks coverage is broader than named peril coverage, as it covers damage from any cause other than those causes that are specifically excluded. As acknowledge in the Lloyd's Report discussed above, all risk policies typically are broad enough to provide coverage for damage caused by a cyber attack unless cyber attack-related losses are specifically excluded elsewhere in the policy. Importantly, under and all risk policy, the policyholder need only prove that a loss occurred. The insurer then bears the burden of proving that an exclusion applies.[53] Moreover, exclusions must be clear and explicit, and will be interpreted narrowly by courts.[54]

As discussed above, in order to trigger business interruption coverage there ordinarily must be physical damage to property caused by a peril that would be covered under the company's insurance policy. Thus, under hypothetical #2, where there is obvious physical damage, if coverage for the property damage is established, coverage for the resulting business interruption should follow once any applicable waiting period has run.

B. If the Loss Results From a Covered Peril, Coverage Will Turn on Whether Any Exclusions Apply

As discussed above, insurers have begun to draft exclusions intended to bar coverage for certain losses due to cyber-attacks.[55] Only a handful of standard form exclusions specifically addressing loss or damage caused by a cyber attack have been introduced in the market. Notably, these exclusions typically are not included in the policy form itself, but instead must be added by endorsement.

---

[53] *See*, *e.g.*, *Kronfeld v. Fidelity & Casualty Co. of New York*, 53 A.D.2d 190, 194, 385 N.Y.S.2d 552, 555 (1st Dep't), appeal denied, 40 N.Y.2d 807, 359 N.E.2d 1002, 391 N.Y.S.2d 1025 (1976) ("The burden is upon the insurer to prove that coverage does not exist. The clause itself must afford clear notice of non-coverage.") (Citations omitted.)

[54] *See*, *e.g.*, *Utica Mut. Ins. Co. v. Prudential Prop. & Casualty Ins. Co.*, 103 A.D.2d 60, 63, 477 N.Y.S.2d 657, 660 (2d Dep't 1984), aff'd, 64 N.Y.2d 1049, 478 N.E.2d 1305, 489 N.Y.S.2d 704 (1985). ("[A]ny limitation in coverage must be described in clear and explicit language.")

[55] *See supra*, page 10, discussing Exclusion Institute Cyber Attack Exclusion Clause (CL 380); Terrorism Form (LMSA 3030); Exclusion Information Technology Hazards Clarification clause; Electronic Data Endorsement A; and Electronic Data Endorsement B.

The most prevalent of these exclusions added by insurers to policies issued to companies in the energy sector is entitled "Institute Cyber Attack Exclusion Clause," which states:

> 1.1 Subject only to clause 1.2 below, in 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.
>
> 1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.[56]

Although this exclusion appears to be broadly worded to exclude all losses resulting from a cyber attack, its reach may in fact be quite limited. As noted above, the insurer bears the burden of showing that an exclusion applies. In order 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." It will be difficult for the insurer to demonstrate the hacker's intent. Moreover, even if a court were to presume that the hacker intended some harm based on the surrounding circumstances, the insurer may be required to show not just that the hacker intended any harm, but that it intended the particular harm that resulted. Additionally, paragraph 1.2 describes an exception the scope of which is unclear, and that could be interpreted to substantially narrow the exclusion.

Other potential exclusions vary greatly in their wording and application given how heavily manuscripted property policies are. As just one illustration, some property policies contain an exclusion for harm, whether "self-inflicted" or accidental, caused by one of the following perils: (1) internet or network failure, (2) corruption of any kind of programming or data, or (3) loss of use/functionality of any software, computer systems, device, and any ensuing inability to conduct business. However, the same exclusion contains an exception for ensuing loss caused by fire, explosion, smoke, or other specified perils. Thus, policies containing such an exclusion would not provide coverage for the damage *directly* caused by the internet or network failure, corruption of programming or data, or loss of use of software or computer systems, but would provide coverage for the likely greater ensuing loss resulting from any of the specified perils. In our hypothetical #2, this exclusion would not apply to the damage caused by the crude oil distillation unit explosion.

Other exclusions may purport to bar coverage for damages due to cyber-attacks using "malware," "computer viruses," or other similar terms. Application of such exclusions will turn on the particular facts of the cyber attack, the language used in the exclusion, and whether the terms

---

[56] Institute Cyber Attack Exclusion Clause, CL380, 10/11/2003

have a commonly accepted meaning or are ambiguous. Illustratively, in hypothetical #1, the hacker installed malware containing malicious code that caused the industrial control system to incorrectly detect errors in remote units even after the units had been fixed, prohibiting the manufacturing process from coming back on line. In contrast, in hypothetical #2, the hacker did not use malware or install any computer viruses, but simply manipulated the operation of the crude oil distillation unit by accessing the industrial control system. Thus, an exclusion for damages caused by cyber-attacks using "malware" or "computer viruses" may apply in hypothetical #1 but not in hypothetical #2.

Finally, insurers may take the position that broad form terrorism exclusions preclude coverage for damage caused by a cyber attack. However, for such an exclusion to apply, the insurer would have to prove that the cyber attack was associated with an act of war or terrorism.

- **Hypothetical #3: The petrochemical refinery explosion described in hypothetical #2 causes widespread pollution**

  The explosion of the crude oil distillation unit and resulting damage to nearby units causes a release of large quantities of crude oil and various distillates onto the policyholder's property.

Nearly all property policies contain some form of a pollution exclusion. However, the scope of these exclusions varies greatly. For example, certain policies bar coverage for:

> any loss, damage, cost, expense . . . which arises from any kind of seepage or any kind of pollution and/or contamination, or threat thereof, *whether or not caused by or resulting from a peril insured* . . . .

In contrast, other policies exclude coverage for:

> Loss or damage caused by or resulting from contamination *unless such loss or damage results from a peril not otherwise excluded*.

Thus, where the contamination is caused by an explosion, such as in the case of the hypothetical crude oil distillation unit explosion, the second form of pollution exclusion quoted above would not apply.

Frequently, there is a question regarding whether the pollution results from one or more than one cause. For example, in hypothetical #3, the contamination arguably was caused by the explosion, as well as the resulting release of crude oil and distillates onto the ground or into waterways. Under these facts, coverage may turn on whether the policy contains so-called "anti-concurrent cause" language, stating that the exclusions apply "regardless of any other cause or event that contributes concurrently or in any sequence to the loss."[57] Where there is no anti-concurrent cause language, coverage may turn on which state's law governs the dispute. In some states, courts have applied the concurrent proximate cause rule, under which there will be

---

[57] *See*, *e.g.*, Business Owner Coverage Form (BP 00 03 07 13), Section I.B.1., p. 17 of 53, Insurance Services Office, Inc., 2012.

coverage where an insured risk and an excluded risk constitute concurrent proximate causes of the loss, as long as one of the causes is covered by the policy. Other states apply the "efficient proximate cause" rule under which the efficient proximate cause is the one that sets other causes in motion which, in an unbroken sequence, result in the loss for which recovery is sought. If the efficient proximate cause is a coved peril, the loss is covered, and if the efficient proximate cause is excluded, there is no coverage.

V. CONCLUSION

Cyber attacks causing large scale property damage and business interruption present a potentially enormous exposure for many large industrial companies, particularly in the energy and infrastructure sectors. This risk is different in kind and scale than the cyber risk most often discussed in the media, among corporate executives, or insurance professionals – privacy related data breaches. While data breaches now occur with such frequency that they have become an anticipated (albeit unwanted and unexpected) loss for most companies, the average cost to a company from a data breach is less than $7 million. In contrast, cyber attacks causing physical damage have more in common with other perils that cause catastrophic losses, such as natural disasters. The risk is ever present, occurrences are infrequent, and the potential losses can be very large. The insurance industry has developed specialized "cyber policies" to cover data breach losses. But these cyber policies do not cover property damage, they are approximately three times as expensive as traditional property policies, and the limits available in the market likely are insufficient to cover a business interruption loss of the magnitude that could result from a cyber attack causing physical to a large industrial operation. That leaves companies to look to their traditional property insurers for coverage.

Surprisingly, many insurers appear to believe that their property policies would not cover such a loss, even absent language that would expressly exclude it. Under the rules governing the interpretation of insurance contracts, the opposite would be true. To the extent property insurers have not included clear language expressly excluding property damage and business interruption losses caused by a cyber attack, policyholders reasonably should expect to be able to obtain coverage. Moreover, even in those instances where insurers have added exclusionary language, whether the exclusion applies will depend upon the specific language of the exclusion and the particular facts of the cyber attack.