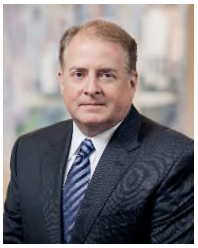
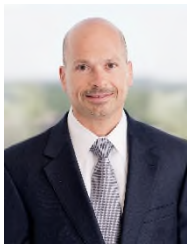
September 11, 2019

Energy Industry: Is Your Insurance Sufficient to Handle a Major Cyber Event?

By Lawrence J. Bracken II, Michael S. Levine and Andrea DeField

Published in Electric Light & Power


This first article in a series of three, on managing cyber risks to the energy industry and gaps in insurance coverage that may adversely affect the energy industry, and others, when responding to a major cyber event.

Earlier this year, the Director of National Intelligence warned that global adversaries, like China and Russia, have conducted cyber espionage to collect intelligence to target critical infrastructure, even warning that "Russia has the ability to execute cyberattacks in the United States that generate localized, temporary disruptive effects on critical infrastructure – such as disrupting an electrical distribution network for at least a few hours" and that "Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage." Office of the Dir. of Nat'l Intelligence, Worldwide Threat Assessment(2019). As these cyber risks increase in frequency and sophistication, it is important to consider your company's cyber risk mitigation and resilience plan.

Insurance is a vital component of any cyber risk mitigation plan. However, insurance policies (even cyber-specific insurance policies) are not created equal when it comes to responding to a cyber event. Corporate policyholders therefore must ensure that their insurance program as a whole is robust enough to cover all potential losses. Below, we address three common gaps in coverage. In our next article, we will cover new insurance products designed to fill these gaps.

Gap 1: Bodily injury or property damage caused by a cyber event

Perhaps the most substantial cyber risk facing power and electric companies is a cyber event that results in physical injury, either to person or property. The risk is real: hackers have tampered with hospital HVAC systems and oil pipeline leak detection systems, deployed ransomware that shut down pharmaceutical production, and taken control of a German steel mill resulting in "massive damage," to list a few examples. The electrical grid is a primary target. In 2016 and 2017, attacks on a Ukrainian electricity provider resulted in widespread outages affecting hundreds of thousands of customers. Just last month, ransomware shut down access to an electrical grid system in Johannesburg.

Unfortunately, most cyber liability policies exclude loss arising out of "Property Damage," often defined as damage to, loss of use of, destruction of, or injury to tangible property. Similarly, cyber liability policies often exclude coverage for bodily injury, including mental anguish and emotional distress. These

exclusions persist even though otherwise covered data breaches involving confidential personal information typically lead to suits alleging, at least in part, these types of damages.

Meanwhile, traditional policies, such as property, pollution liability, and general liability policies, may contain cyber exclusions—likely creating a major gap in your insurance program for cyber-related risks. The Insurance Services Office (ISO), which develops form language for commercial general liability policies, has issued endorsements that limit or eliminate coverage for property damage or bodily injury arising out of a cyber event or data breach, including coverage for damages arising out of disclosure of confidential information and the loss of, loss of use of, damage to or inability to access electronic data. In the United Kingdom, insurers often exclude coverage for loss or damage arising out of the use of a computer to inflict harm.

Even where the policies do not contain an express cyber exclusion and are silent on coverage for damage or loss caused by a cyber event, there is uncertainty that is likely to lead to litigation over whether the loss is covered. Insureds therefore should carefully review all potentially responsive policies to determine whether their program contains this cyber coverage gap.

Gap 2: Coverage for fines and penalties

With the push for smart meters and smart grids, energy companies are collecting big data, which in turn means greater opportunity for breach or disclosure of protected information and greater regulatory risks in the event of a breach or disclosure. Many state and federal regulators, and their foreign counterparts, have developed laws or regulations governing privacy breach disclosure. Failure to comply with these regulations can lead to massive fines and penalties. For example, the European Union's General Data Protection Regulation (GDPR), which governs the handling of personal data of individuals in the European Union, dictates fines of up to 10 million EUR or two percent of a company's worldwide annual revenue, whichever is higher, for certain infringements; and up to 20 million EUR, or four percent worldwide annual revenue, for more serious infractions. The California Consumer Privacy Act (CCPA), which becomes effective on January 1, 2020, imposes statutory damages of the greater of $100 to $750 per California resident and incident, or actual damages, in class actions arising out of a major data breach (as well as civil fines). Cyber liability and other insurers frequently deny coverage for such penalties and statutory damages, arguing that they are uninsurable as a matter of law.

Gap 3: Coverage for business income losses

What happens if you and your customers are unable to access your system, resulting in significant lost business income due to a cyber event? Or, what if your system is not the target of a cyber attack, but there is an attack on a key vendor, supplier, customer or service provider such as a cloud storage provider, and you are unable to operate your business as usual? These are just a few of the numerous cyber risk scenarios that can impact your bottom line.

While cyber insurance policies typically cover first-party costs, such as costs to investigate and remediate an actual or suspected cyber breach, and third-party costs, such as defense expenses arising out of a lawsuit against your company, not all cyber policies provide coverage for lost income as a result of a cyber event. For an additional premium, however, many cyber insurers will offer coverage for business income losses arising out of a cyber event, such as a security failure/cyber attack, system failure, or network failure. This coverage is typically subject to a time-based deductible called a waiting period,

meaning that the coverage does not kick in unless and until the interruption has lasted the waiting period's designated hours. In addition, some cyber insurers now offer this coverage to include situations where it is not your network or system that is inaccessible, but that of a vendor on which your business relies. This coverage, called contingent or dependent business interruption coverage, is a key component of a robust cyber insurance program.

Conclusion

These are only three of the many gaps that could be exposed by a cyber event. In our next article in this series, we will cover how to fill these gaps with new insurance products and/or endorsements to your existing policies. In the final article in the series, we will provide guidance on purchasing adequate limits for your cyber-related coverage.

The risk that a cyber event will impact your business is substantial and likely inevitable. However, through a robust insurance program, your company can partially mitigate the impact of a cyber event.

Lawrence J. Bracken II *is a partner in the insurance coverage practice in the Atlanta office at Hunton Andrews Kurth LLP. Lawrence has more than 30years of experience litigating and investigating insurance coverage, class action, technology, environmental and commercial matters. He can be reached at +1 404 888 4035 or lbracken@HuntonAK.com.*

Michael S. Levine *is a partner in the insurance coverage practice in the Washington, DC office at Hunton Andrews Kurth LLP. Michael's has more than 20 years of experience litigating insurance disputes and advising clients on insurance coverage matters. He can be reached at +1 202 955 1857 or mlevine@HuntonAK.com.*

Andrea DeField *is an associate in the insurance coverage practice in the Miami office at Hunton Andrews Kurth LLP. Andrea finds risk management, risk transfer and insurance recovery solutions for public and private companies. She can be reached at +1 305 810 2465 or adefield@HuntonAK.com.*