

ANDERSON KILL

Cyber Insurance Alert

Ransomware Attack on Colonial Pipeline Underscores Multiplicity of Cyber Risks and Potential Insurance Coverages



By Joshua Gold

Key points:

The severity of ransomware attacks continues to escalate, and the potential damage extends far beyond the ransom paid

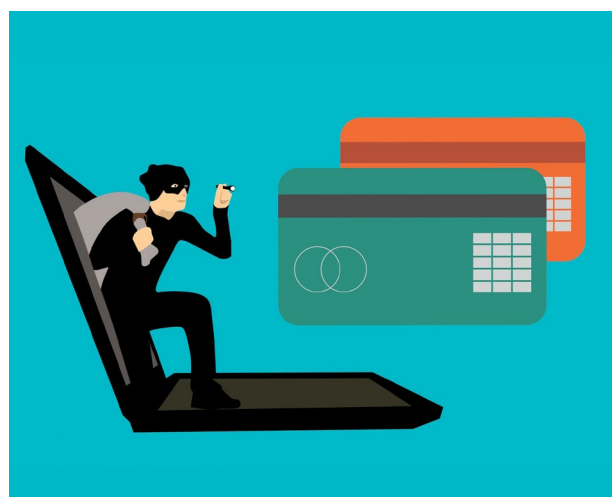
In addition to cyber insurance policies, traditional insurance policies may respond to losses and liabilities stemming from a ransomware attack

After a ransomware attack, policyholders should err on the side of inclusiveness when notifying their various insurance companies

The hack on the Colonial Pipeline is but the latest in an unrelenting string of serious ransomware attacks. Once upon a time, ransomware, while serious, was more of annoyance for organizations wherein a payoff of \$5,000 to \$30,000 often was enough to obtain return of system control and data access.

From 2017 on, however, the trend has become decidedly worse for cyber crime targets. Ransomware has become an ever escalating game of high-stakes cyber theft, system paralysis, and data exposure. During the pandemic, hackers aimed their attacks on some of our most crucial sectors, including health care. As the New York Times reported last fall, cyber attacks on hospitals and health systems “have become their own kind of pandemic.”

While the stakes have escalated, many policyholders should be able to find insurance coverage for some of their most significant ransomware losses, not only under a specialty cyber policy, but also under crime insurance or all-risk property coverage.



Ransomware Takes On New and More Dangerous Dimensions

While ransomware demands have exploded, the ransom demand is not the only harm inflicted on organizations. Systems can be permanently damaged and data files corrupted or compromised. As is the case with many recent ransomware attacks, the cyber gang targeting the Colonial Pipeline went after a critical industry with the hope that they would have no choice but to pay an enormous ransom. Further, the hacking gang, DarkSide, used

tools that enabled them to steal corporate data, thus opening up yet another cyber risk exposure to the organization.

All Insurance Policies Have to Be On-Deck With a Serious Cyber Incident

Most cyber insurance policies expressly promise coverage for cyber extortion payments. Thus, policyholders should have insurance coverage for the ransoms they pay, the forensics that must be employed following an intrusion, and the fees and costs required to interface with regulators, law enforcement, and other stakeholders. Additionally, many cyber insurance policies promise to cover not just extortion payments, but also business interruption losses after a cyber attack (including a ransomware attack). As such, if the ransom is not paid (or even if it is paid but the hacker still refuses to relinquish control of systems and data), then the policyholder should be able to seek business income coverage above the retention amount.

While cyber insurance undeniably is an important insurance policy in the current environment, it is not the only option for insurance protection for cyber-related perils. Insurance coverage for losses stemming from ransomware exist under other insurance policies as well. In a recent pro-insurance coverage ruling, the Indiana Supreme Court found that crime insurance can cover ransom payments (see our [March 24 Alert](#) for a detailed discussion).

In that case, *G&G Oil Co. of Indiana, Inc. v. Cont'l. W. Ins. Co.* the policyholder was victimized after a hacker installed “malicious computer code that renders the victim’s computer useless by blocking access to the programs and data.” After consulting with law enforcement,

the policyholder paid \$35,000 of bitcoin to the hacker and sought coverage under the computer fraud insuring provision under the crime section of its package business policy. The insurance company denied the insurance claim, and the policyholder sued. Although the Supreme Court of Indiana could not resolve the case entirely, it did reverse the lower courts’ rulings for the insurance company and held that the ransomware caused a “direct loss” to the policyholder and would constitute a covered claim if further evidence indicated that the ransomware was injected into the computer system using some form of trickery. This case is also a lesson that policyholders should engage a computer forensics specialist that can analyze the attack and the methods used by the hacker to gain access.

Another decision from last year indicates that policyholders can also have property insurance coverage for damage to systems and loss of data as a result of ransomware. In *Nat’l Ink & Stitch, LLC, v. State Auto Prop. & Cas. Ins. Co.* (D. Md. Jan. 23, 2020), the court held that a policyholder that suffered serious damage and losses from a ransomware attack was entitled to all-risk property coverage for lost data, lost software, and a dysfunctional computer system and hardware. The court held in relevant part that:

Here, not only did Plaintiff sustain a loss of its data and software, but Plaintiff is left with a slower system, which appears to be harboring a dormant virus, and is unable to access a significant portion of software and stored data. Because the plain language of the Policy provides coverage for such losses and damage, summary

...err on the side of being overinclusive when choosing which insurance companies to notify after discovering a cyber incident.

judgment will be granted in favor of Plaintiff's interpretation of the Policy terms.

In light of these and other decisions, policyholders should recognize that when confronted with a cyber attack, there may be insurance coverage under more than one insurance policy line. Indeed, it may be that beyond first party coverage, the policyholder will have (and need) third-party liability coverage for claims made when ransomware exfiltrates data, or where investors, customers, clients, regulators, or law enforcement claim against the policyholder in the wake of a malware attack. As such, D&O insurance, E&O insurance, CGL coverage, EPLI policies, and excess insurance must be considered, among other policy forms.

Further, it is safer to provide the earliest notice of claim you can and err on the side of being overinclusive when

choosing which insurance companies to notify after discovering a cyber incident. Even insurance company underwriters have indicated to us that this would be their approach if they were in the shoes of a policyholder confronting a serious cyber incident. Sound cyber risk management requires no less. ▲

JOSHUA GOLD is a shareholder in Anderson Kill's New York office and is co-chair of the firm's Cyber Insurance Recovery Group. Josh has represented corporate and non-profit policyholders in various industries, with recoveries for his clients well in excess of \$1.5 billion. His practice involves matters ranging from data security, international arbitration, directors and officers insurance, business income/property insurance, commercial crime insurance, admiralty, cargo, and marine insurance disputes.

jgold@andersonkill.com
(212) 278-1886

***We are
interested in
your feedback
on topics for
future articles
and seminars.
Please email
us.***

About Anderson Kill

Anderson Kill practices law in the areas of Insurance Recovery, Commercial Litigation, Environmental Law, Estates, Trusts and Tax Services, Corporate and Securities, Antitrust, Banking and Lending, Bankruptcy and Restructuring, Real Estate and Construction, Foreign Investment Recovery, Public Law, Government Affairs, Employment and Labor Law, Captive Insurance, Intellectual Property, Corporate Tax, Hospitality, and Health Reform. Recognized nationwide by Chambers USA, and best-known for its work in insurance recovery, the firm represents policyholders only in insurance coverage disputes – with no ties to insurance companies and has no conflicts of interest. Clients include Fortune 1000 companies, small and medium-sized businesses, governmental entities, and nonprofits as well as personal estates. The firm has offices in New York, NY, Stamford, CT, Newark, NJ, Philadelphia, PA, Washington, D.C. and Los Angeles, CA.

This publication was prepared by Anderson Kill P.C. to provide information of interest to readers. Distribution of this publication does not establish an attorney-client relationship or provide legal advice. Prior results do not guarantee a similar outcome. Future developments may supersede this information. We invite you to contact the editor, Joshua Gold at jgold@andersonkill.com or (212) 278-1886, with any questions.