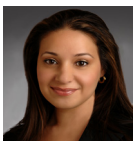
ANDERSON KILL
Cyber Insurance Alert

Ransomware and Malware Attacks in the News: Insurance and Risk Management Implications

By Joshua Gold and Luma Al-Shibib

Key points:

Ransomware, malware and other cyberattacks continue to hit the news.

Coverage for cyber losses is often available under a variety of insurance policy types.

Be prepared not only to prevent cyberattacks, but to move swiftly to limit losses when they occur.

Serious cyber perils continue unabated for almost all organizations and computer users. While ransomware is by no means the only dangerous cyber risk exposure, it continues to plague many policyholders with its ability to impede, if not shutter, operations.

In the last several days, there have been three significant developments involving ransomware and malware attacks. Some of the news was good and some was not.

New Developments in Ransomware Incidents

First, it was reported early this month that a California law enforcement department was able to regain control of its systems after a security compromise. Last month, a hacker infiltrated the San Bernardino County Sheriff's Department's computer system and disrupted access to the department's systems. The hacker secured a $1.1 million ransom, which was partially paid under the county's cyber insurance coverage. According to the Associated Press, the malware attack prevented authorized access to "a system that provides information on whether a person is wanted for crimes elsewhere in the county."

Second, the city of Dallas is presently dealing with a ransomware attack that is impeding police, fire, and medical dispatch. The effects of the malware have been ongoing for several days and obviously imperil action-critical services that protect life and overall public safety. The city has not yet said whether it has paid any ransom or negotiated with the hackers as the city has been able to restore some of its computer systems.

Third, a recent decision from a New Jersey appeals court re-affirmed that a war risk exclusion in a property insurance tower could not be used to

thwart coverage for pharma giant Merck for $1.4 billion in losses stemming from a malware infection, inserted in the global NotPetya attack of 2017, that spread to 40,000 Merck computers. The insurance companies had argued that the malware was attributable to Russia and triggered the exclusion for war and hostile acts, based on allegations that the Sandworm hacking group within the GRU Russian military intelligence organization had unleashed the malware globally in 2017. The appellate panel rejected the insurance companies' coverage argument and held that "this was not hostile or warlike action, and applying this exclusion would be inappropriate."

The New Jersey decision is especially welcome news to policyholders after a disappointing property insurance decision from the Ohio Supreme Court at the end 2022 involving insurance protection against ransomware loss. In ***EMOI Servs., L.L.C. v. Owners Ins. Co.***, Ohio's high court ruled that damage to software did not constitute "direct physical loss or damage."

Cyber Perils Include Ransomware and Much More

Ransomware is not the only cyber threat that demands attention. Indeed, some security incidents involve no hacker at all. It was just revealed, for example, that the LAPD may have inadvertently disclosed the identities of undercover law enforcement officers combatting drug cartels.

When vigilance fails, all is not doom and gloom. As illustrated above, policyholders may have insurance coverage to pay for malware attacks, ransoms, and other security incidents that lead to losses and third-party claims. Furthermore, some policyholders are able to recover from ransomware attacks without paying a ransom, which is especially good news for a host of reasons.

Bottom line: Make sure you are up to date understanding the cyberattack vectors used by hackers, and take all prudent steps to secure systems and data (including data that is mobile and data that is hosted on third-party platforms).

Action Items After Hacking Occurs

When a hacker strikes, be prepared to move methodically through all of the steps needed to address the security incident, including but not limited to:

- Contact law enforcement, including the FBI, promptly.
- Provide prompt notice to all potentially relevant insurance companies, including those from whom you hold policies including cyber, crime, property, D&O, inland marine, and CGL coverage.
- Before paying a ransom, make sure to comply with Treasury Department guidance concerning the transfer of money to those who may be on the OFAC SDN list. The Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists prohibits in most instances "U.S. persons" from dealing with anyone who appears among a "list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific."
- Work closely with a seasoned computer forensics firm to determine the level and scope of the security breach. Remember that more recent malware strains have the ability to not only en-

Policyholders may have insurance coverage to pay for malware attacks, ransoms, and other security incidents that lead to losses and third-party claims.

crypt data, but to exfiltrate it as well, thus potentially leading to a privacy event as well as loss of access to computer systems and data.

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

LUMA S. AL-SHIBIB *is a shareholder in the New York office of Anderson Kill and is co-chair of the firm's Cyber Insurance Recovery Group. Luma focuses her practice on insurance recovery for corporate policyholders, with an emphasis on directors & officers liability insurance and cyber liability insurance. She has successfully assisted clients in recovering cyber-related losses under their cyber liability insurance, commercial crime insurance, and all-risk first party property insurance policies.*
lal-shibib@andersonkill.com
(212) 278-1048

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, Wills, Trusts and Estates, 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, Newark, NJ, Philadelphia, PA, Washington, D.C., Stamford, CT, Los Angeles, CA, Denver, CO, and Boston, MA.