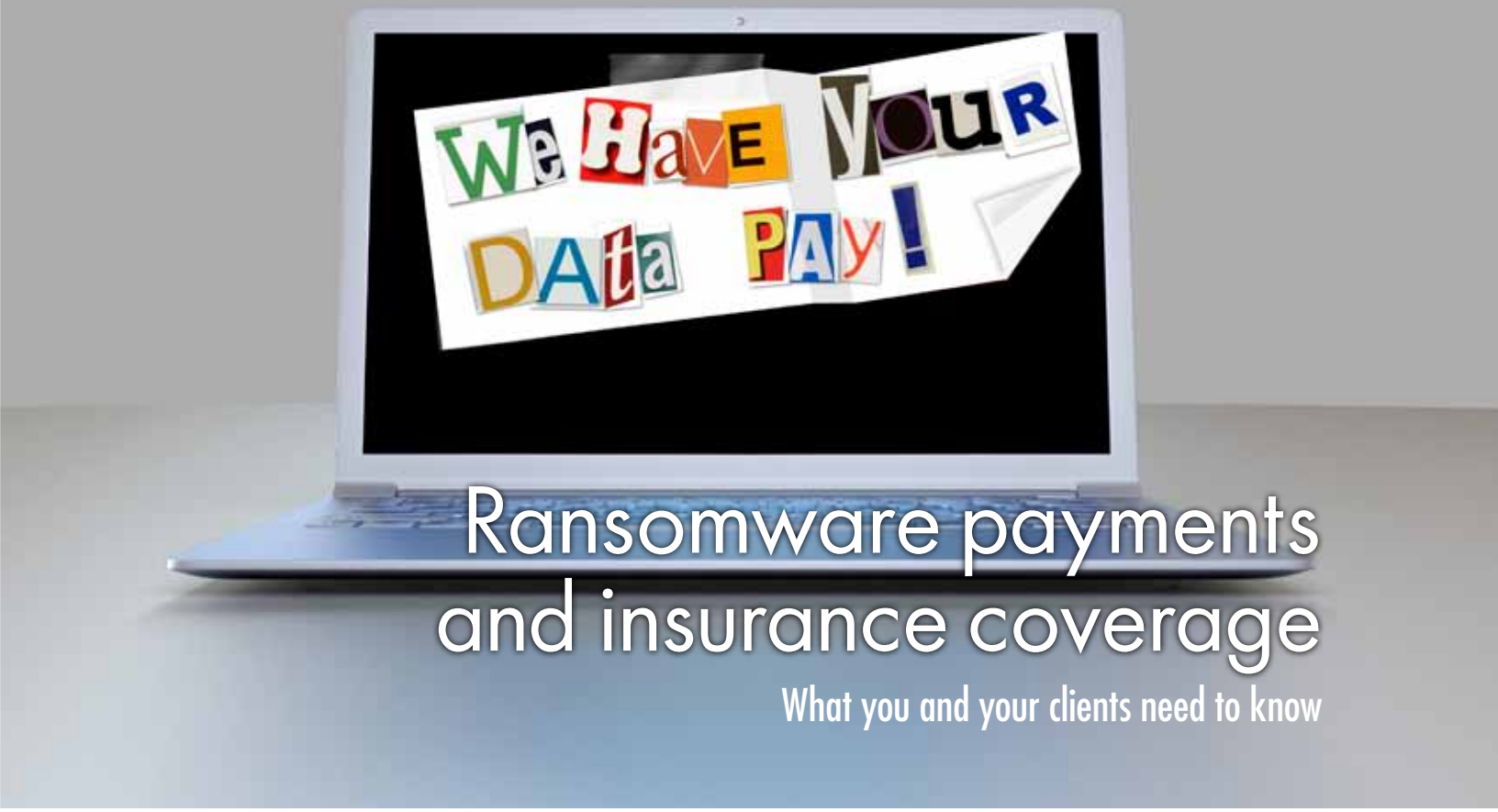
—Reprinted with permission from PIA Management Services Inc.—

ERIC B. STERN AND ANDREW A. LIPKOWITZ
Kaufman Dolowich & Voluck LLP



Ransomware payments and insurance coverage

What you and your clients need to know

The increasing prevalence of ransomware attacks impacts the role of insurance in covering such losses. It also impacts agents who are procuring policies to anticipate the coverage issues that may arise from such events.

Ransomware is a form of malware (i.e., malicious software that gets installed on a computer without the user's consent and is harmful to the computer) in which the access to important data and computer systems are locked or encrypted, unless the victim agrees to pay a ransom to regain access. According to a recent study by Recorded Future, a cyber security firm, there were 230 attacks against municipalities during the first three quarters of 2019. For example, last summer the school district in Rockville Centre, N.Y., paid $88,000 in ransom after its data was affected by a ransomware attack.

As the number of ransomware attacks has risen, so have the number of claims reported to insurance companies involving these attacks. AIG announced in May 2018 that, of all the cyberclaims it received in 2017, ransomware was the largest cause of loss, making up 26% of the cyberclaims that it received that year. By comparison, the next largest cause of loss was data breaches caused by hackers (12% of all claims received).

The decision regarding payment of a ransomware demand is a complex one, which becomes even more layered when there is coverage for the loss. This article will examine some of the issues faced by insurers and insureds in dealing with a ransomware attack and provide guidance for evaluating insurance coverage options. In addition, this article also will discuss the role of professional insurance agents in the process of protecting against the risk of ransomware attacks.

Associated risks

While ransomware attacks continue to become more frequent, according to the FBI these attacks also are becoming more targeted, sophisticated and costly. Such attacks often are spread through unsolicited email phishing campaigns or vulnerabilities in a victim's cyber security systems. According to Beazley, ransomware attacks increased 105% in the first quarter of 2019, compared to the first quarter 2018—while the average

ransom demand increased by 93%, to $224,871. There were a total of 1,493 ransomware incidents in 2018 according to the FBI's internet crime report.

We focus our discussion on recent examples of ransomware attacks against municipalities and public-school districts. This is because such entities have become frequent targets of attacks as many do not have the resources to establish sophisticated cyber security protections. Further, such entities are required to disclose information related to attacks publicly, including the role of any insurance coverage. Conversely, private companies are not necessarily required to disclose to the public when they have been impacted by a ransomware attack. In fact, private companies have incentive to avoid publicly disclosing ransomware attacks, the presence of coverage for such attacks, and their responses to the attacks in order to avoid any potential negative impacts on their business and/or future attacks.

The targets of the attacks are faced with not only the difficult work in recovering from the attack, but the consequential decision of whether to pay the ransom that is demanded, or whether to refuse to pay in favor of working around the problem. Indeed, the U.S. government does not encourage ransom payment because it does not necessarily guarantee the release of the seized system back to the impacted user, and, further, it may lead to later attacks.

As an example of an agreement to pay ransom leading to a further attack, the Wolcott, Connecticut school district was hit in June of 2019 with a ransomware attack in which hackers blocked access to part of the school district's computer system. The Wolcott hackers demanded a $12,000 ransom payment in order to restore access. The Walcott town council voted and announced to allow payment of up to $9,999 in ransom to the hackers. However, before the payment was made, the school district was hit with a second attack in September of 2019. The second attack occurred less than 10 days after the public announcement of payment.

By contrast, as noted above, Rockville Centre school district paid $88,000 in ransom following the attack on its systems, which was covered by the district's insurance company in excess of the $10,000 deductible. In addition, according to news reports, the district's IT director was able to shut down the attack before it affected all of the district's data. Apparently, this allowed the school district's insurance company to negotiate a lower ransom payment, from $176,000 to the $88,000 that

actually was paid. Despite the negotiation and ultimate payment, there are no reports of subsequent attacks.

While ransom-payment demands can be costly, it may be even more costly to refuse to meet the hackers' demands—both in terms of the costs to restore service as well as the cost of having operations interrupted for an extended period of time. As an extreme example of the cost of working around the ransomware, Baltimore reportedly lost at least $18.2 million due to a ransomware attack that shut down important municipal services in May 2019. The $18.2 million in costs are a combination of both lost or delayed revenue and direct costs to restore Baltimore's systems. The amount of loss reportedly suffered by Baltimore is substantially more than the $76,000 in ransom that the hackers demanded.

According to reports, Baltimore was not insured for this loss. However, it was reported in October 2019 that Baltimore is purchasing $20 million in cybercoverage. Reportedly, the coverage will include costs to respond to a ransomware attack, including coverage for business interruption losses.

New York's capital, Albany, was hit with a ransomware attack in March 2019. Albany declined to pay the ransom, and it did not reveal how much in ransom was demanded by the hackers. The city claimed that it was able to avoid paying the ransom because it had backed up its critical systems daily. Despite Albany's reported preparedness for the attack through daily backups, the decision cost Albany approximately $300,000. According to news reports, the costs included upgrading security software and replacing the destroyed servers.

Ransomware coverage options

The options for cyber security insurance, specifically for ransomware coverage, vary amongst insurers. Such policies may provide reimbursement for ransom payments made in response to a ransomware attack, as well as the costs to conduct a forensic investigation to determine the validity, cause and scope of the cyberthreat, and/or reimburse or make ransomware payments. A ransomware policy also may cover the costs to evaluate the system post-ransomware attack to identify vulnerabilities, however, insurers typically will not cover the costs of upgrading the system. As the Rockville Centre example demonstrates, involving the insurer early on in the process of responding to a ransomware attack has its benefits, as Rockville Centre's insurer was able to negotiate a lower ransom payment.

The key question in responding to the demand in a ransomware attack is identifying the process for making the controversial decision of whether to pay a ransom demand or suffer the costs of a work-around. The decision to make a ransom payment is controlled by different factors (i.e., costs of work-around, risk of further attacks, precedent setting or the risk of incomplete recovery)—many of which are weighed differently by insurers and insureds. Because of this, it is in the best interests of both insurers and insureds to delineate the powers of decision making to avoid conflict should a ransomware attack occur during the policy period.

Insurance agents and brokers with expertise in this area have a critical role to play in advising businesses and organizations about the risks of ransomware attacks and explaining the terms of the policies. Agents and brokers should work to outline the decision-making process at the time of policy purchase. Different insurance policies have taken different approaches. Some policies explicitly require the insured's consent to make any ransom payment. Conversely, some policies allow the insured to control the decision, subject to the insurer's consent.

Agents and brokers also can be instrumental in negotiating the coverage terms of a cyberpolicy, and in ensuring that such policies provide coverage for loss as well as the necessary resources to respond to a ransomware attack.

The decision-making process with respect to payment of ransomware demands should be part of a larger response plan constructed in light of relevant state cyber-security laws, such as the New York SHIELD Act, which contain notification requirements following a data breach. Such response plans should include contingencies for all data attacks and should be made in coordination with qualified data privacy law firms.

Be aware of the risks

As ransomware attacks continue to spread, it is important for insurance companies, agents and insureds to be aware of the increasing risk that such attacks pose, and the policy solutions for how to deal with them before the attacks occur to avoid conflict and protect the insurer and the insured.

Stern is a partner and co-chair of the Data Privacy & Cybersecurity Practice Group at Kaufman Dolowich & Voluck LLP. Lipkowitz is an associate at Kaufman Dolowich & Voluck. His primarily focuses is insurance coverage litigation and monitoring.