KAUFMAN | DOLOWICH

Mansfield Rule Certified 2022-2023

Insurance coverage options before ransomware attacks, *PropertyCasualty360*

By Eric Stern, partner and co-chair of the Data Privacy & Cybersecurity Practice at Kaufman Dolowich & Voluck LLP, and Andrew A. Lipkowitz, attorney at KD in Woodbury, NY
PropertyCasualty 360 | August 22, 2019

In the case of a ransomware attack, insurers and insureds need to understand which party decides whether such payments are to be made.

Computer systems everywhere have become the targets of ransomware attacks in recent years. Ransomware is a form of "malware" (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 to the affected computer system or data. AIG announced in May 2018 that of all the cyber claims it received in 2017, ransomware was the largest cause of loss, making up 26% of the cyber claims that it received that year. By comparison, the next largest cause of loss was data breaches caused by hackers, at 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 examines some of the issues faced by insurers and insureds in dealing with a ransomware attack and provides guidance for evaluating insurance coverage options.

Recent ransomware attacks against municipalities

The targets of ransomware attacks are forced to confront a difficult and consequential decision: 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 doesn't encourage payment of ransom. Payment of a ransomware demand may not lead to release of the seized system back to the impacted user and may lead to further attacks. As a recent example of payment and further attacks, according to reports, in March 2019 the court system of Jackson County, Georgia, paid attackers $400,000. A few months later, in June 2019, the Administrative Office of the Georgia Courts was the victim of another ransomware attack. Currently, this latest attack is still ongoing so the ultimate outcome is not known.

Conversely, not paying the ransom can sometimes be even more costly — both in terms of the costs to restore service as well as the cost of having operations interrupted for an extended period of time.

To illustrate the costs of this difficult decision, in mid-2019, two municipalities took two different approaches to the question of payment of ransom. One widely reported ransomware attack in May 2019 affected the city of Baltimore's servers, blocking access to important municipal services, and preventing city employees from accessing emails. Baltimore's city government refused to pay the ransom that the hackers demanded (13 bitcoins, which at the time was the equivalent of approximately $76,000), and the impact from the attack is still ongoing months later.