The Debate over Ransomware Insurance: Should it be prohibited?

7.29.2021

Last year, nearly a quarter of all cyber incidents worldwide involved ransomware attacks, including attacks on businesses, schools, government agencies and critical infrastructure. These attacks have generated a debate over whether, and under what circumstances, ransomware victims should be able to look to their insurers to reimburse ransom payments.

Today about half of all U.S. businesses have cyber insurance policies, many of which cover payments of ransom to cyber extortionists. However, there is a growing reluctance among some insurers to cover such payments. The trend is for insurers to closely examine their insured's cyber security systems and procedures—and decline to issue coverage for ransom payments if they find those systems lacking. And some insurers now refuse to provide such coverage regardless of their insureds' ability to resist cyber attacks. Last May, for example, AXA—one of the world's largest insurers—announced it would no longer sell ransomware coverage in France. AXA is likely to extend this prohibition to other countries, and other major insurers are expected to follow suit.

Insurers and insureds are also becoming increasingly wary of making ransom payments if by doing so they risk incurring the wrath of government agencies or insurance regulators. Last October the U.S. Treasury Department issued a warning that individuals and businesses—including insurance companies—that facilitate the payment of ransom could be violating anti-money laundering and sanctions regulations. FBI Director Christopher Wray recently told Congress: "It is our policy, it is our guidance from the FBI, that companies should not pay the ransom." The New York Department of Financial Services (DFS) echoed that sentiment, warning that the epidemic of ransomware attacks threatens to jeopardize the stability of the financial services industry. At least three states—New York, Pennsylvania and North Carolina—are considering legislation

Related People

Eric J. Flessland
Shareholder

Related Services

Cybersecurity and Privacy Specialty Team

that would ban state and local government agencies paying ransom in response to demands from cybercriminals.

Because payment of ransom remains legal in this country—at least for now—no U.S. business has yet to be penalized by the government for doing so. However, the strong opposition of some government officials and insurance regulators to such payments, which they believe only encourages cybercriminals to launch more ransomware attacks, has created much uncertainty in the insurance industry.

Not everyone in the industry believes ransomware insurance is a bad thing. The American Property Casualty Insurance Association (APCIA) has addressed this issue at length in its Cyber Extortion/ Ransomware Guiding Principles. The APCIA says that insurers "must be able to provide reimbursement coverage for the policyholder's payment of ransom for cyber extortion." The Association argues that many businesses simply have no option but to pay ransomware demands; their failure to do so can cause their financial ruin.

The lack of coverage for ransom payments, claims APCIA, would penalize small businesses who can't afford to make those payments without insurance. Such a ban would also, in the opinion of some insurance experts, actually encourage ransomware attacks—shifting the focus of cyber criminals to the highest value targets where an interruption would do the most damage to society. Some in the insurance industry also argue that ransomware insurance actually prevents cyber extortion because insurers will insist that insureds in the market for such insurance have rigid safeguards in place to prevent cyber attacks. Conversely, the argument goes, businesses that do *not* have ransomware insurance will not be appropriately diligent in implementing procedures and systems to prevent such attacks.

On the other hand, opponents of cyber ransom point to evidence that malware gangs are focusing their attacks on businesses that have ransomware insurance. An interview last March of a notorious member of a cyber extortion gang known as REvil bears this out. REvil, also known as Sodinokibi, runs a rasomware-as-a-service operation, in which developers sell malware to affiliates who use it to lock up an organization's data and devices. The gang member revealed that his organization has lately taken to hacking into insurance companies to identify their policyholders who have ransomware insurance. REvil then sets out to hack into those policyholders' networks and extort ransom payments from them.

In sum, whether or not payments to ransomware gangs should be insurable has become a hotly debated topic that has divided the insurance industry and government regulators. How this issue will be resolved remains to be seen. Because those favoring a prohibition on ransomware coverage appear to be gaining the upper hand, insureds would be wise to assume that such coverage will be hard to come by in the future—and implement measures to prevent the increasingly sophisticated malware attacks of bad actors like REvil.

Thomas Bick
202.454.2818
bick@butzel.com

Eric Flessland
313.983.6901
flessae@butzel.com