BEECHER CARLSON

RANSOMWARE AND MARKET REACTION

BY: CHRIS KEEGAN AND OREN WORTMAN

The increase in ransomware attacks over the last two years has been dramatic. Costs of attacks and payments have increased significantly, and the sophistication of the malware has increased.

⇧ **239%** — Ransomware claims increased 239% from 2018 to 2019

⇧ **228%** — Cost of ransomware payments increased 228% from 2018 to 2019

⇧ **31%** — Average ransomware payments increased 31% from Q2 2020 to Q3 2020

⇧ **3x** — Ransomware payments in 2019 were 3 times as large as the 2018 payments

⇧ **4x** — 4 times more extortion demands were paid in 2019 than in 2018

⇧ **22%** — Ransomware incidents where data had been exfiltrated increased from 8.77% to 22% from Q1 2020 to Q2 2020

What are the markets doing?

The markets are reacting to these developments by increasing premiums and seeking to provide tools to help insureds better identify and correct vulnerabilities. Insurers are also focusing on a more careful selection of their policyholders.

To date, the insurance market has not limited coverage for cyber-attacks, but there have been adjustments in premium to cover the increased losses. Insurance carriers target increases of 0-5% rate in Q2 2020, 5-15% in the Q3 2020, and rising to 10-30% by the end of the year. Not all increases are in this range, but cyber insurance buyers should be prepared for requests at these levels. Some adjustments to the structure of programs, such as raising retentions, can be made to limit the increased costs.

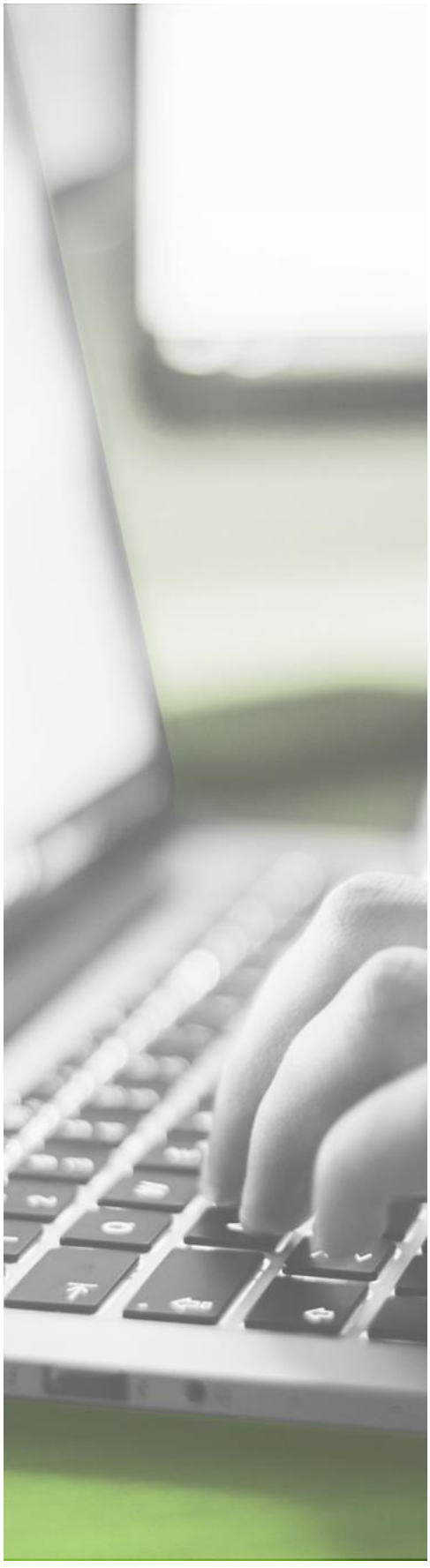
Recent announcements from the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) do not change reporting or other requirements but emphasize that regulators have increased vigilance and may pursue civil fines and penalties. A review of the OFAC and FinCEN fine lists do not show fines due to ransomware payments.

The insurance market has seen only a small minority of situations where payments have been held up because of an indication that the payments might be made to OFAC and FinCEN restricted entities.

1. There are only a handful of known threat actor groups or individuals listed on the known Specially Designated Nationals ("SDN") lists in addition to a short list of sanctioned nation states (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).
2. Further, there are very few instances where attribution can be made with a degree of certainty. Many businesses will not be able to get enough information on attribution before a decision is made on payment and will be taking a risk to get their businesses operating.

Most payments where insurance companies are involved are made through specialist ransomware negotiation and incident response (IR) companies with experts in negotiations with threat actors. The Bitcoin wallets of these companies are usually the source of the payment – though a small number of cyber insurance companies have their own in-house experts and wallets. If the payments are small enough, they can be made on credit. These are typically backed by the guarantee of the insurance company or the insured. As it is the IR firm that has the best knowledge of the threat actors, the insurance companies rely heavily on their expertise and on the investigation done by them for confirmation that they are in compliance with OFAC, FinCEN, and any other payment regulations. The service-level agreements (SLA) with the IR companies will often stipulate that it is their responsibility. Insurers will also be looking to breach counsel and their insured for confirmation. If criminal investigations are taking place, the agency may also provide information on the threat actors receiving payment.

Attribution and enforcement of the OFAC and FinCEN rules may become more difficult due to moving from Bitcoin to other crypto currencies that provide greater anonymity. Tactics, techniques, and procedures (TTPs), which are typically used for attribution, are also becoming increasingly shared with the rise of ransomware as a service. Ransomware criminals are eager to remove roadblocks to payment and go to great lengths to preserve their anonymity using frequently rotated burner cryptocurrency wallets. To date, we have not seen companies in the insurance industry, or their vendors, seek to get a license from Treasury for an exception to OFAC rules for payment of ransomware.



Most cyber insurance policies do not have specific exclusions for payment of ransomware that might be subject to OFAC and FinCEN restrictions but incorporate provisions that freeze the effect of the policy and make it subject to OFAC oversight in the event an entity or person claiming the benefits of the policy has violated any sanctions law. Insurance companies have indicated that they will be reluctant to act if that action is illegal, as it could affect their licensing or subject them to fines and penalties. That said, our experience is that cyber insurance companies are honoring their contractual obligations and paying claims. The exception has been a few cases where there is clear evidence of payment to a banned entity. In those cases, the insureds, banks, and IR firms are all under the same restrictions.

We recommend that companies have proper business continuity and disaster recovery plans in place that are regularly tested so that payment of ransomware is not the organization's only choice. Backups of critical systems should be segmented and stored offline. Companies should have a well-documented and ransomware-specific incident response plan to allow clear and efficient decision-making to weigh legal risks against the risks to the business.

Chris Keegan leads the Beecher Carlson Cyber and Technology Practice and places network, privacy, technology, and media E&O insurance for companies in a variety of industries including financial institutions, authentication providers, manufacturers, healthcare, retail, and telecommunications companies. He has also executed cyber information risk assessment projects and worked with regulators on evaluation of E-Business risks. He can be reached via email at ckeegan@beechercarlson.com or by phone at 646.358.8530.