BEECHER CARLSON

PART OF THE BROWN & BROWN TEAM

RANSOMWARE TRENDS IN 2020 AND HOW TO PLAN FOR 2021

BY: JESSICA SLATER

A wide array of unique cyber incidents emerged in 2020 including supply chain attacks, COVID-19 related phishing attempts, and a staggering increase in ransomware attacks. Most significantly, the way that threat actors operate, how they attack, and their demand amounts escalated significantly in 2020. As a result, the cyber insurance market[1] is reacting strongly to mitigate loss impact. This response is expected to continue in 2021.

Here, we focus specifically on how the ransomware spike in 2020 impacted the cyber insurance market and will, consequentially, impact how ransomware coverage is evaluated and quoted going forward in 2021. To position your company for the most favorable ransomware coverage terms, it is important to partner with your broker well in advance of renewal to assess and proactively address your company's specific risk.

Ransomware Trends

In the US alone last year, frequency of ransomware attacks increased by more than 100%. COVID-19 contributed to this trend due to the exploitation of increased corporate reliance on Remote Desktop Protocol (RDP) with an expanding number of employees working remotely. In addition to exploiting unsecured RDP endpoints, attackers continued to target known vulnerabilities present in corporate Virtual Private Network (VPN) appliances and use email phishing schemes; however, the dramatic increase in ransomware can be attributed to the changes in the profile of threat actors carrying out the attacks and a significant increase in the sophistication of the tactics, techniques, and procedures they are using to do so.

Targeted Attacks

Historically, ransomware attackers were semi-sophisticated, individually creating ransomware and performing 'spray and pray' attacks. In 2020, essentially turning ransomware into a highly organized business, advanced attackers monetized by focusing on targeted attacks against larger organizations with the means to pay higher ransom demands and established a ransomware-as-a-service infrastructure that threat actors leverage to carry out a ransomware attack in exchange for payment, likely a portion of the ransom. This means that the attacks were sophisticated and could be performed by a larger set of threat actors very quickly.

[1] https://beechercarlson.com/company-literature/2021-cyber-market-update/

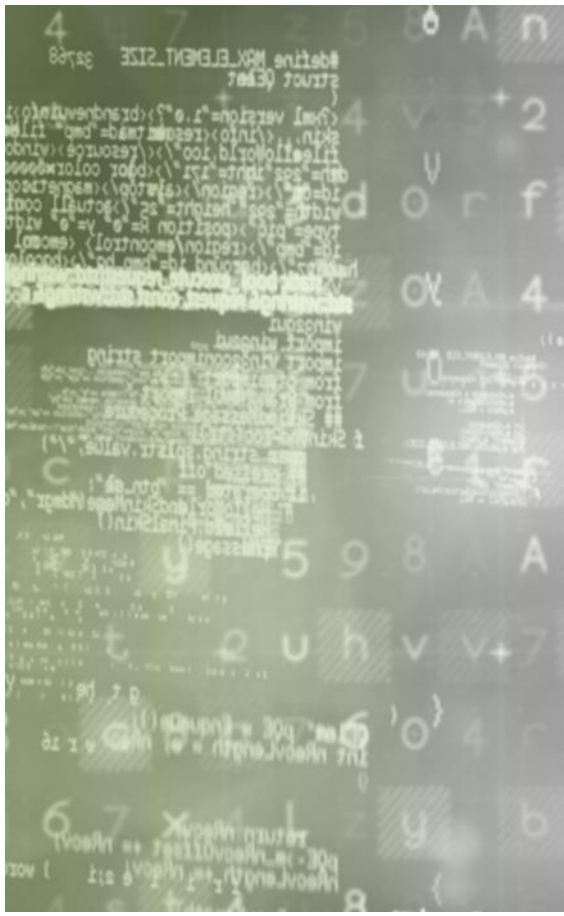
Double and Triple Extortion Approach

One ransomware trend that gained traction in 2020 was the double and triple extortion approach. Double extortion attacks function like previous ransomware attacks that blocked access to a company's crucial systems and data through encryption, but with an added element – attackers also threaten to leak sensitive information if the ransom is not paid. Triple extortion attacks add the additional element of a Distributed Denial of Service attack to prolong the Business Interruption impact and make it more difficult to execute on disaster recovery strategies. It is estimated that in 2020, more than 1,000 companies had information leaked following a ransomware attack.[2] Double and triple extortion is expected to accelerate in 2021 as a prominent strategy used by cybercriminals.

Threat Actors Researching Their Target

Not only did the frequency of attacks increase as threat actors shifted their approaches, but the severity of the ransom amounts they demanded surged. Last year, there were multiple ransom payments in excess of $1,000,000. In 2020, the average ransom demand was more than $100,000, which was approximately a 33% increase compared to the fourth quarter of 2019.[3] Now that cybercriminals are treating ransomware as a commoditized item, they will spend time performing research on a victim's financial status and attempting to discern how much cyber insurance a company purchases when determining their ransom demand amount. There was, however, a notable decrease in the average ransom demand in December that may be a result of fewer victims paying the demand. Despite these companies choosing not to pay, profit margins remained high for ransomware actors and the risk of sanctions remains low.

Ransomware Insurance: Industry Impact and Market Responses



In 2020, the cyber insurance market experienced continued negative loss trends, particularly with respect to ransomware. As a direct result, in 2021, insureds can expect market reactions to include closer examination in the application and placement process, upward pressure on premiums and retentions, reduced capacity, and more restrictive terms.

Following the substantial increase in ransomware attacks, the cyber insurance industry is reconsidering how they evaluate ransomware risks. Some markets are including additional questions in their applications or are requiring a completed ransomware supplemental in addition to the application. At the application and placement process, carriers are carefully examining each company's level of cyber maturity from a control perspective with a specific emphasis on ransomware preventative controls and controls that enhance resilience in the face of an attack. There has been a noticeable increase in the use of external vulnerability and attack surface scanning tools by insurance underwriters, both during the evaluation phase and throughout the policy period.

In order to mitigate loss impact, some markets may require a sublimit of liability or may even request co-insurance for certain coverage, including ransomware.

[2] https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2021-will-be-year-extortion
[3] https://www.upguard.com/blog/what-is-ransomware-as-a-service#:~:text=Ransomware%20as%20a%20service%20(RaaS)%20is%20a%20subscription%2Dbased,of%20each%20successful%20ransom%20payment

How Companies Can Prepare

When faced with a challenging cyber insurance market, companies that are well prepared for underwriting meetings and the placement process obtain the best results. This includes the following:

- Demonstrating a proactive approach to addressing emerging attack trends
- Eliminating known attack vectors and vulnerabilities exposed to the internet
- Implementing a layered approach to the application of security controls – 'Defense in Depth'
- Providing thoughtful and thorough responses to the questions on insurance applications and supplements

With assistance from their brokers, companies should identify underwriter concerns early in the process and involve their IT teams to proactively address those concerns to the extent possible. To ensure a company's specific risk is being addressed appropriately, companies should review their risk appetite and compare that to appropriate available limits and retentions. From a financial perspective, several large carriers have expressed the intent to increase premium in 2021, making it prudent for companies to prepare their budgets with these increases in mind. Companies can also consider creative risk financing approaches such as captives and alternate or integrated risk vehicles.

To proactively address these market trends, Beecher Carlson is engaging with current and prospective clients to provide guidance. This includes in depth preparation workshops, identifying open vulnerabilities of concern, and advanced modeling to ensure adequate limits and policy coverage.

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 EBusiness risks. He can be reached via email at ckeegan@beechercarlson.com.

Oren Wortman leads the Cyber Advisory team, helping customers better understand their maturity and risk exposures and enabling them to make quantifiable and fact-based decisions relative to cyber risk treatment. He has specific subject matter expertise in information security, technology and cyber risk management, conducting cyber maturity and regulatory assessments, governance, and overall security program development. He can be reached via email at owortman@beechercarlson.com.