Cyber insurance claims explode in severity

by Bethan Moorcraft 26 Apr 2021 Insurance Business Magazine

Ransomware is a dominant source of concern in the cyber insurance community today. In recent years, there has been a significant uptick in the frequency and severity of ransomware attacks, impacting businesses of all sizes and in all sectors. Hackers have grown more sophisticated and targeted in their attacks, aiming for larger organizations that can afford bigger ransoms. As a result, cyber insurance claims have exploded in severity.

“A couple of years ago, we saw very few ransomware claims, and if we did, the demands were typically around $8,000, $10,000, or maybe $30,000 at the higher end,” reflected Tamara Ashjian, Director of Claims, Tokio Marine HCC – Cyber & Professional Lines Group. “Paying the ransom was the rational decision as it would be considerably more expensive for the insured to be out of operation, incurring business interruption losses and/or other expenses to recreate digital assets.”

But the cyber landscape changed in 2018 with the arrival of the Ryuk ransomware – a lucrative and targeted malware designed for “big game hunting” within enterprise environments. With the ability to encrypt network drives, essential files and systems, attackers using Ryuk started asking for substantially larger ransom amounts. By mid-

2019, threat actors were routinely deploying targeted ransomware attacks and demanding six-figure ransoms – often in the $500,000-600,000 range – for the release of systems and data.

"We thought the mid-six-figure demands were high at the time," said Ashjian. "Little did we know ransom demands were going to explode in 2020. Last year, we saw several very complex strains of ransomware, which were extremely damaging to insureds' systems, and several of the ransom demands were ludicrous. The highest demand we saw in 2020 was $50 million. On average, even after the payments have been negotiated down, insurers still have to pay anywhere between $3 million to $5 million in these more targeted and sophisticated attacks."

In 2020, a new wave of ransomware attacks hit the market. These individuals were known as 'double extortion' threat actors and were able to maximize their probability of making a profit by threatening the victim with an additional abuse of the information they encrypted, such as selling or auctioning it.

"These threat actors are spending a significant amount of time in the insured's systems, gathering valuable information before they deploy the ransomware," explained Ashjian. "We've started to see claims where hackers show proof that they have stolen information and threaten to publish that information unless specific demands are met in addition to the ransom."

Historically, companies have been advised to maintain secure data back-ups to reduce any downtime, business interruption, and data recovery costs associated with a cyberattack. While back-ups are still critically important, ransomware strains have grown so complex that they're now able to encrypt back-up systems, leaving insureds to shore up their cyber defenses in other ways.

"The number one way that hackers gain access to insureds' systems is via employee error or negligence," Ashjian told *Insurance Business.* "Threat actors typically gain access to a network through a phishing scheme, where the employee receives a spoof email or call and is tricked into providing their credentials. Multi-factor authentication (MFA) is a critical mitigation tool that adds a layer of defense against phishing attacks, but now we're seeing claims where the hackers are able to bypass the MFA to gain access."