CYBER UPDATE

CHITTENDEN GROUP
INSURANCE

Ransomware Attacks Reach All-time High in Q4 2020: Spotlight

Ransomware attacks spiked in 2020 as the fear and chaos of COVID-19, combined with the transition to remote work, provided an abundance of opportunities for cybercriminals. Advisen data shows ransomware attacks reached an all-time high in 2020, with a particular emphasis on manufacturing companies.

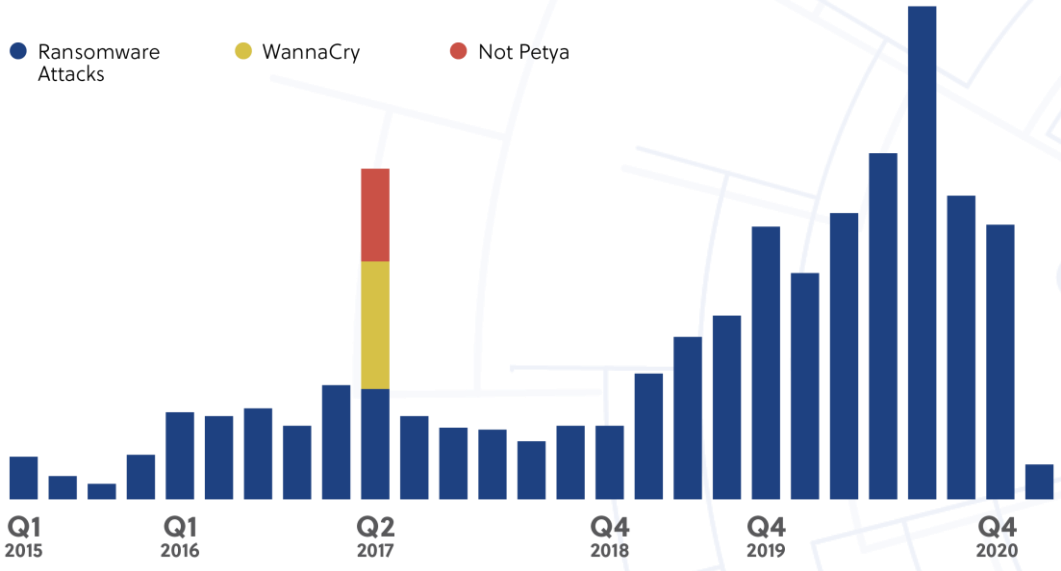
Advisen's loss database shows ransomware attacks in Q3 2020 were on par with the number of ransomware losses in Q2 2017—driven by the global WannaCry and NotPetya attacks—before rising to the highest frequency on record in Q4 2020. The decrease in ransomware attacks in Q1 2021 may be due to a data lag and is not indicative of a real decrease in the frequency of attacks. These numbers will increase with our continued data collection efforts.

Health care, manufacturing and public administration accounted for half of all ransomware attacks in 2020 and the beginning of 2021. This is a shift from 2019 when public administration and educational services were the dominant industries facing ransomware attacks. In 2018, public administration and health care saw the greatest frequency of attacks, according to Advisen loss data.

Business interruption losses arising from these attacks can be quite severe, leading some companies to pay extremely high ransoms in order to make their businesses operational once more.

For example, Hexion—an American chemicals company—was hit with a ransomware attack in March 2019, causing the entire global network to shut down. The company incurred $17 million in loss costs related to the incident, according to Advisen loss data.

Ransomware Attacks, Frequency



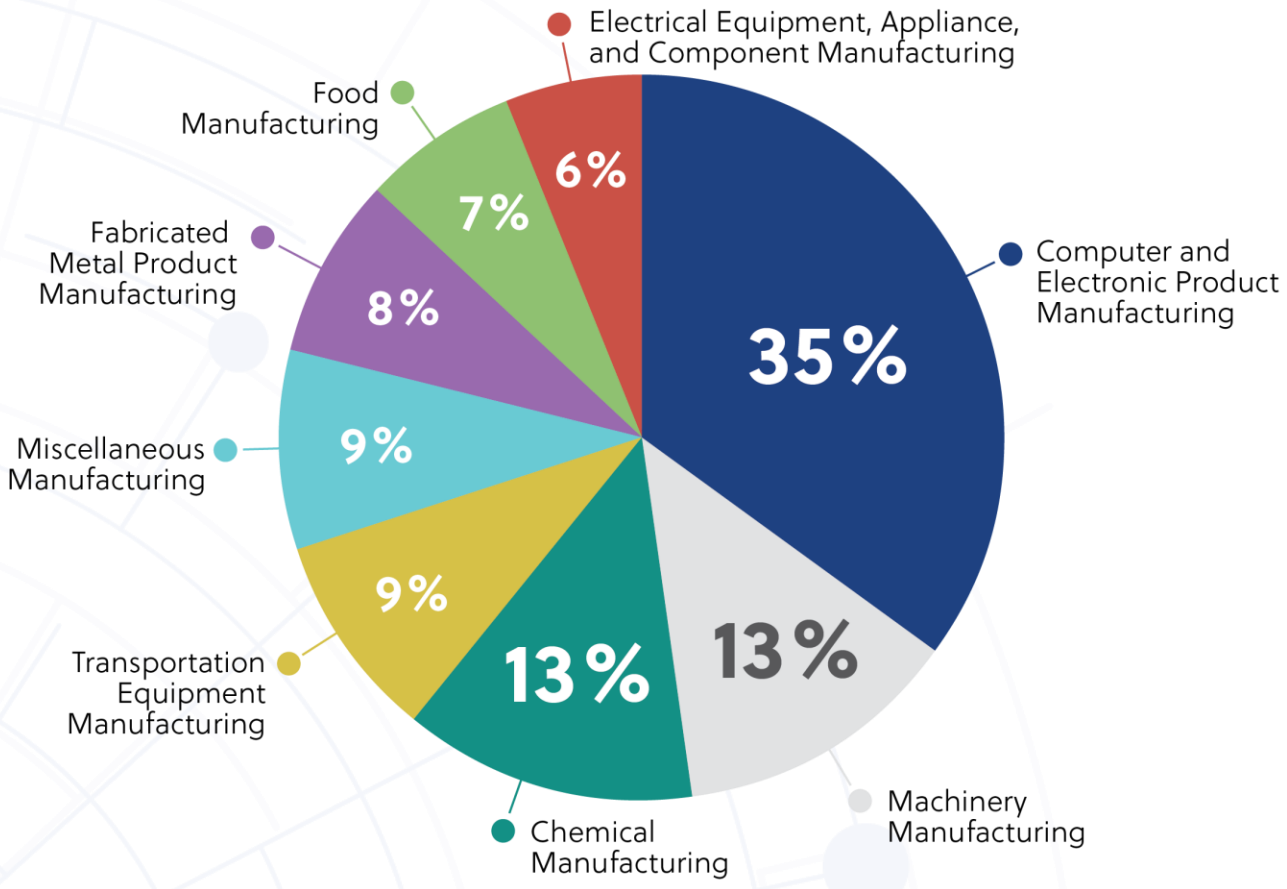
The high frequency of manufacturing ransomware attacks in 2020 is unprecedented in Advisen's loss database, accounting for more than double the frequency of ransomware attacks seen in all prior years (including the WannaCry ransomware attacks in 2017).

Looking at ransomware attacks at manufacturing companies in 2020, Computer and Electronic Product Manufacturing accounted for the greatest percentage of losses. This industry includes electronic chip-makers, laptop makers and weapon manufacturers, among others.

For example, a major electronics manufacturer for defense and communications, Communications & Power Industries (CPI), was taken offline by a ransomware attack and forced to pay a ransom of around $500,000, according to Advisen loss data. CPI makes components for military devices and equipment, like radar, missile seekers and electronic warfare technology.

Machinery manufacturing and chemical manufacturing each accounted for 13% of the remaining ransomware attacks in 2020. Machinery manufacturing companies that faced ransomware attacks in 2020 include drilling product manufacturers, bath manufacturers, and industrial robot manufacturers. Chemical manufacturers that faced ransomware attacks in 2020 include pharmaceutical manufacturers, developers of medical technology, and a gene manufacturing company, according to Advisen.

Manufacturing Ransomware Attacks, 2020, Frequency



**Advisen's loss data is curated from a wide variety of public sources. Our collection efforts focus on larger and more significant cases. For this reason, the figures in this article may not be fully representative of all cases of this type.*