CYBER UPDATE

PELNIK INSURANCE

Critical Infrastructure Cyberattacks on the Rise

Critical infrastructure cyberattacks are increasing in frequency according to Advisen's loss database, and some experts are worried the worst is yet to come.

There are sixteen industry sectors in the United States that make up the country's critical infrastructure. These sectors are considered so vital their incapacitation or destruction would have a debilitating effect on national security, economic security and/or national public health and safety, according to the United States' Cybersecurity and Infrastructure Security Agency (CISA). Poisoned water supplies, opened dam floodgates and pipeline spills are a few of the many worst-case scenarios that could result from a cyberattack on critical infrastructure. The sectors that have been designated as critical infrastructure include the following:

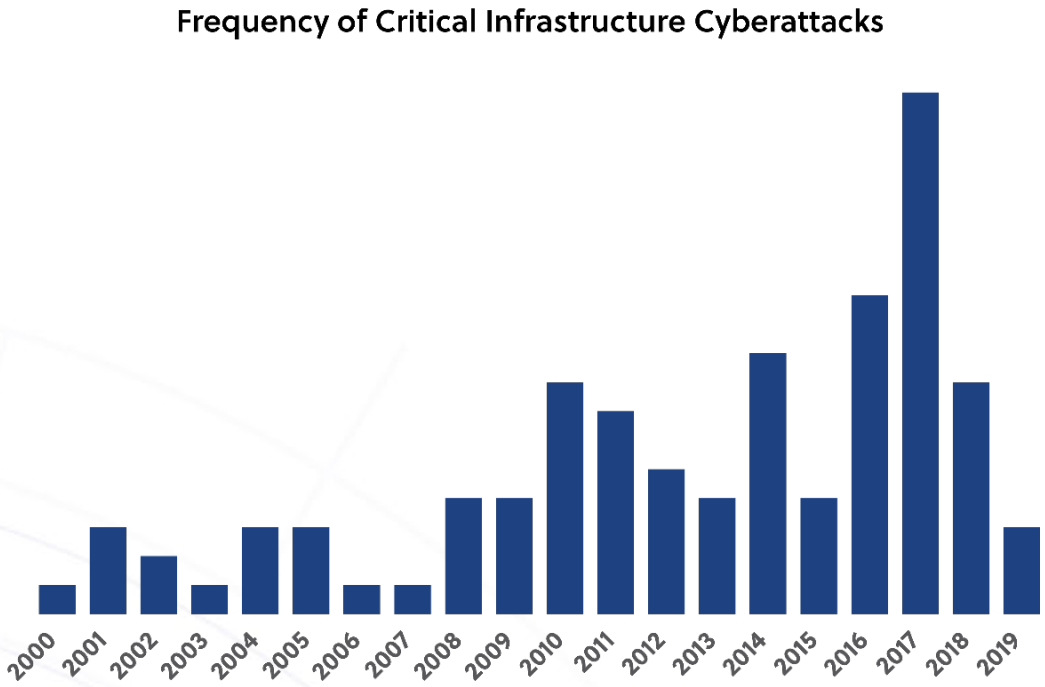
- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Health care and public health
- Information technology
- Nuclear reactors
- Materials and waste
- Transportation systems
- Water and wastewater systems

Further, recent critical infrastructure attacks in Advisen's loss database include:

- A ransomware attack in June 2021 on JBS meatpacking temporarily shut down all operations. The meatpacking company—which processes roughly one-fifth of the nation's meat supply—paid an $11 million ransom to become operational again.
- A ransomware attack on the Colonial Pipeline, the nation's largest fuel pipeline, occurred in May and temporarily shut down all operations, causing a temporary increase in gas prices in the United States. The Colonial Pipeline paid nearly $5 million in ransom to restore operations, although some of the ransom was later recovered, according to Advisen loss data.

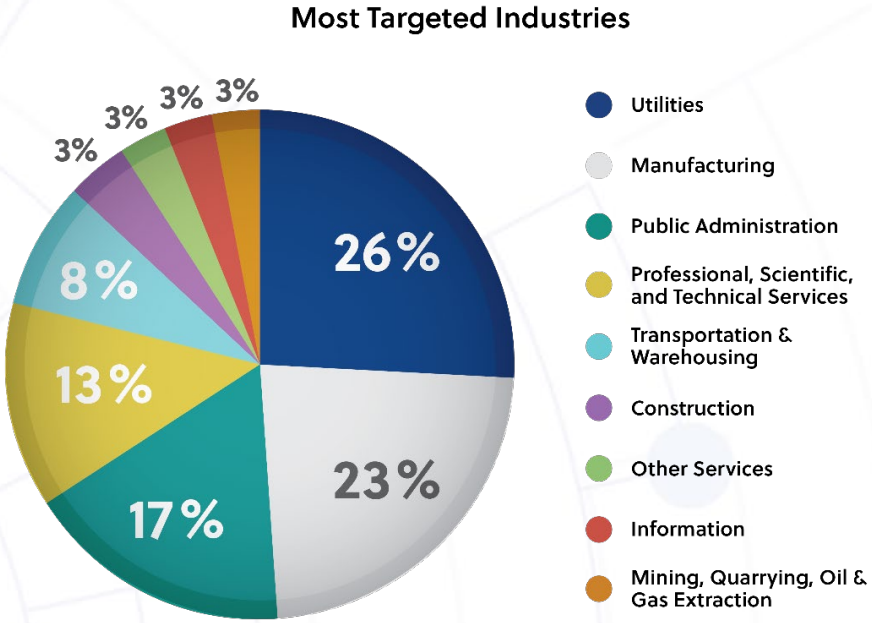
- Hackers briefly attempted to increase the levels of sodium hydroxide to a lethal amount as part of a February cyberattack on a water treatment plant in Florida. The plant operator quickly noticed the increase in sodium hydroxide levels and lowered it to the original amount, preventing anyone from being harmed, according to Advisen loss data.

Frequency of Critical Infrastructure Cyberattacks



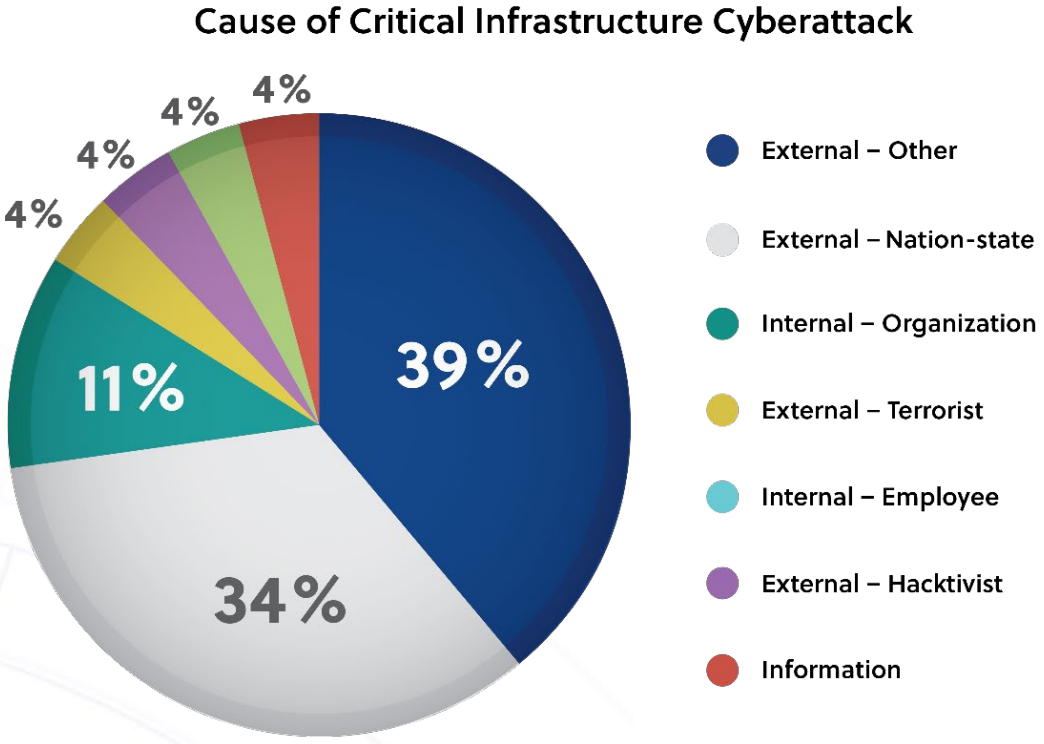
Source: Advisen

Unfortunately, cyberattacks on critical infrastructure are becoming increasingly common. Since 2008, the frequency of cyberattacks on critical infrastructure has been trending upwards, according to Advisen loss data. The drop-off in 2019 is likely due to a data lag and is not reflective of an actual decrease in frequency.



Source: Advisen

Looking specifically at the sectors designated as critical infrastructure, the utilities sector was the most frequent target of cyberattacks – accounting for 26% of total losses, according to Advisen loss data. Manufacturing had the second-highest percentage at 23%, followed by government entities (shown AS PUBLIC ADMINISTRATION) at 17%.



Source: Advisen

The vast majority of critical infrastructure cyberattacks come from external sources. Unidentified external hackers account for the greatest percentage of these attacks at 39%, followed by nation-state attacks at 34%, according to Advisen data. These attacks typically involve malware.

**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.*

Pelnik Insurance

100 Ridgeview Dr, Suite 100
Cary, NC 27511

www.Pelnik.com
919-459-8000