In recent times, ransomware has become an alarming threat across the globe. Like many other industries, the manufacturing industry is also a major target of cybercriminals. According to a November 2020 [report](https://www.dragos.com/blog/industry-news/manufacturing-sector-cyber-threats/) by security company Dragos, the number of ransomware attacks in the manufacturing industry tripled during the year. Although a large part of manufacturing industry relies on information technology, it also relies largely on Industrial Control Systems for mass production of goods. This is the area that cyber criminals actively seek to target.

With the [recent ransomware attack](https://www.theverge.com/2021/5/10/22429433/colonial-pipeline-cyber-security-ransomware-attack) on one of the largest oil pipelines of United States, many gas stations had no choice but to shut down – causing national gas prices on average to rise above $3. To resolve the matter, Colonial Pipeline [had to pay](https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom?sref=ExbtjcSG) $5 million ransom within a few hours. Though, earlier the opposite of this was reported by CNN and Reuters, the ransom payment news was also later confirmed by the [Wall Street Journal](https://twitter.com/dnvolz/status/1392948690294345730).

This news is worrisome since the success of a large-scale ransomware attack can be encouraging for the hackers to launch future attacks. Particularly for the manufacturing supply chain, if one element gets affected due to a cyberattack, it can lead to a chain of consequences.

For instance, if a manufacturing facility producing medicines or health products is hit by ransomware, it can have negative impact on the whole healthcare sector.

In another instance last week, the world’s largest meat processing company JBS [was targeted](https://www.bbc.com/news/world-us-canada-57318965) by a well-planned ransomware attack, where computer networks were hacked and operations were shut down across Australia, US and Canada. JBS has 47 facilities in Australia. It has the largest production facility network in the country. Though the operations have now restored, the incident raises a very important question about preparedness against cyber attacks in the manufacturing industry.

Threat researcher John Hultquist of security company FireEye says, "The supply chains, logistics, and transportation that keep our society moving are especially vulnerable to ransomware, where attacks on choke points can have outsized effects and encourage hasty payments."

According to a [report](https://www.zscaler.com/resources/white-papers/threatlabz-ransomware-review.pdf) by the research team at ThreatLabZ in May 2021, companies in the manufacturing industry are the biggest targets of double-extortion ransomware attacks. In a double-extortion attack, criminals steal data alongside encrypting it. ThreatLabZ indicates that 12.7% of the companies affected by double-extortion attacks worked in the manufacturing sector, followed by the services, transport, technology, and retail industries. In another [2021 Global Threat Intelligence Report](https://hello.global.ntt/ja-jp/newsroom/ntt-global-threat-intelligence-report-2021) by NTT, the manufacturing industry saw 300% increase in worldwide cyber attacks

# Why are Hackers Targeting Manufacturers?

The industry makes a profitable target for cybercriminals particularly because it involves operations that cannot be kept out of action for longer time periods. Hence, the affected organization tends to give in easily to the demands of the attackers and pay huge amounts as ransomware compensation, mostly in the form of [cryptocurrency](https://www.zdnet.com/article/how-bitcoin-helped-fuel-an-explosion-in-ransomware-attacks/).

Another reason for quick response is that the losses a company can incur as a result of downtime are sometimes more than the ransom amount. Hence, the manufacturers may be more inclined towards paying the attackers. What makes this even further attractive to the cyber criminals is the fact that the industry does not primarily focus on cybersecurity operations which makes it easy and profitable target for hackers.

Due to the nature of manufacturing processes, often the networking and industrial assets are exposed to the internet. This provides opportunities to cyber gangs to access the network remotely via technologies such as VPN and Remote Desktop Protocol (RDP), or unpatched vulnerabilities in a system.

# How can Manufacturers Adopt a Secure Approach?

Considering the statistics of increased attacks, it’s still not late for industrial manufacturers, particularly food, pharmaceuticals, chemical and automotive sectors to take necessary steps against future attacks. For this, we need to adopt three basic measures such as:

1. Adopting a Cybersecurity Framework

By adopting best cybersecurity practices and complying with standards, manufacturers can control their production and reputation. Manufacturers can follow any of the cybersecurity frameworks such as NIST, IEC 72443, or NIS. These frameworks provide best practices to facilitate security by keeping all manufacturing process in line such as inventory asset management and threat identification.

1. Improving Network and Operational Visibility

Your IT team must be updated about your inventory. If they are not aware of the exact number of devices on the network, it’s not possible to provide better resiliency. It’s common for manufacturers to have wrong estimate of their devices. When all the assets are correctly identified on the network, it provides visibility in real-time to all the devices, their communication, connections, and protocols. This allows for continuous monitoring, spotting and troubleshooting issues related to communication and network troubleshooting, since system deviation often indicates network attacks.

1. Integrating IT and OT Network Security

Operational Technology helps meet production targets while Information Technology addresses networking and cybersecurity issues. By integrating IT and OT, operations can become more resilient by reducing security risks around tightly connected Industrial Control Systems.

# Preparing for an Attack

Apart from taking steps to decrease the likelihood of an attack, manufacturers also need to be prepared for a time an actual attack occurs. For a company in manufacturing industry, a ransomware incidence response plan should answer these questions

* How much downtime is acceptable and what impact will downtime have on operations?
* What are the available resources for investigating and mitigating a threat after it has already occurred?
* What is the insurance coverage to help deal with the impact of ransomware attack, including the payment and operational interruption?

To know more about how you can secure your manufacturing business from evolving cyber threats, get in touch with KMTech [today](https://kmtech.com.au/contact-us/).