CYBER RISK

MANUFACTURER RANSOMWARE ATTACKS CAN BE DEVASTATING

RANSOMWARE ATTACKS on manufacturers are increasing, and criminals are becoming adept at shutting down production for days, weeks and even months, costing the victimized firms millions of dollars in lost production and sales interruptions.

As cybercriminals grow more sophisticated, manufacturers have become one of their favorite targets. Modern factories rely on interconnected production equipment, industrial control systems and enterprise software to keep operations moving. When those systems are compromised, the effects can ripple throughout an entire organization.

The threat is especially severe for small and midsize manufacturers. While large companies may have the financial resources to withstand an extended shutdown, such a disruption could become an existential threat to smaller operations.

A month without production can mean lost customers, broken supplier relationships, cash flow problems and, in some cases, the end of the business.

Recent attacks illustrate just how disruptive ransomware and related cyberattacks have become.

Jaguar Land Rover: Five-week production shutdown

A cyberattack on Jaguar Land Rover's information technology systems forced the company to halt production for five weeks in 2025 at its major manufacturing facilities in the U.K. The disruption affected approximately 5,000 suppliers, logistics providers and other businesses tied to the company's operations.

Cost: Estimated at $2.5 billion, making it one of the costliest cyber incidents ever to affect a manufacturer. After production resumed, the company worked for months to restore systems and stabilize its supply chain.

Clorox: Production, distribution disrupted for months

A ransomware attack on Clorox's information technology systems in August 2023 forced the company to take portions of its network offline, disrupting manufacturing, order processing and product distribution across North America.

The firm temporarily reverted to manual processes while it rebuilt critical systems, resulting in widespread shortages of products such as bleach, disinfecting wipes and trash bags on retail shelves.

Cost: $356 million in reduced sales and $49 million in direct costs related to response and recovery efforts. The company also incurred expenses during the months-long process of restoring automated systems and rebuilding inventories.

Dole Food: Ransomware halts production, shipments

A ransomware attack in February 2023 forced Dole Food Co. to temporarily shut down production at several North American facilities and suspend food shipments while it contained the incident. The attack disrupted operations, causing temporary shortages of packaged salads and other produce at grocery stores.

Cost: Approximately $10.5 million in costs associated with the attack, including lost revenue, recovery expenses and operational disruptions during the quarter in which the incident occurred.

How it happens

Cybercriminals increasingly spend time inside company networks before launching an attack.

They identify critical systems, steal sensitive information and learn how an organization operates. Some threat actors even search for cyber insurance policies to understand coverage limits and tailor ransom demands accordingly.

They may also threaten to release stolen data publicly if a ransom is not paid, creating additional legal, regulatory and reputational risks.

Steps manufacturers can take

- Require multifactor authentication for all critical systems.
- Regularly back up production and business data and test restoration procedures.
- Segment manufacturing systems from business networks to limit the spread of an attack.
- Train employees to recognize phishing attempts and other social engineering tactics.
- Promptly install security updates for all software and have processes in place to monitor networks for unusual activity.
- Develop and regularly test incident response and business continuity plans.

Finally, manufacturers should review their cyber insurance coverage.

A robust cyber insurance policy may help cover losses and expenses related to forensic investigations, legal services, business interruption, system restoration, notification and other costs associated with recovering from a cyber incident.