A RECENT CYBER ATTACK IS CAUSING A SHORTAGE OF CLOROX PRODUCTS.



The cyber attack that hit the cleaning products manufacturer Clorox in August is still affecting the supply of the products to customers

The Clorox Company is a multinational consumer goods corporation with a focus on the development and marketing of numerous products for personal, professional, and home cleaning as well as for health and hygiene.

The manufacturer of household cleaning products revealed in mid-August that it had experienced a cybersecurity incident and had been forced to shut down some of its systems.

Unauthorized activity on a few of The Clorox Company's information technology (IT) systems has been discovered. The company stated in an 8-K filing that it started acting to stop and cease the activity as soon as it became aware of it. This included putting some systems offline.

The Company is collaborating with law enforcement while working diligently to respond to and remedy this situation. In order to continue providing its clients with services, Clorox has established workarounds for some offline operations to the greatest extent practicable and in accordance with its business continuity strategies.

The business has taken some of its systems offline in response to the cyberattack while it implements extra "protections and hardening measures to further secure them."

To bolster its investigation and ascertain the extent of the issue, Clorox has contacted top third-party cybersecurity specialists. Clorox also informed law police. It is unclear at this moment whether the attackers have taken any company data.

The business also disclosed that, in order to keep providing its clients with service, it has put in place workarounds for some offline processes.

The business noted that the incident has disrupted its business operations and is anticipated to do so going forward.

Although the corporation withheld information about the attack, the way it handled the situation indicated it was a ransomware attack. No extortion organization has yet claimed responsibility for the attack on the Clorox Company.

The business submitted a fresh 8-K form to the US Securities and Exchange Commission (SEC) this week. Due to the steps it has taken to resolve the situation, the company confirmed that the incident was contained.

According to the information currently available, the company thinks that the unlawful activity has been stopped thanks to the measures it has taken to deal with the problem. the 8-K form is read. "A large section of the company's IT infrastructure was affected by the cyberattack, which severely disrupted Clorox's business activities. In addition to fixing the infrastructure, the company is reintegrating the systems that were taken offline proactively. The week of September 25 is when the company anticipates starting the process of returning to regular automated order processing. The vast majority of Clorox's manufacturing facilities have already started producing again, and the company anticipates that the ramp-up to full output will take some time. The Company is unable to predict when things will return to normal in full at this time.

The magnitude of the financial and business effect of the security breach is still being assessed, according to Clorox. Order processing still experiences delays, and there are still significant amounts of product outages. The company anticipates a significant impact on Q1 financial results.

Given the ongoing recovery, "it is premature for the Company to determine longer-term impact, including fiscal year outlook." carries on the form.