

# RKON Case Study

*RKON Recovery  
Saves Business from  
Costly Data Loss*



## PROJECT NAME:

Ransom

## INDUSTRY:

Food & Beverage  
Services

## SOLUTION NEEDS:

Ransomware  
Recovery

## FOR MORE INFORMATION:

 328 S. Jefferson, Suite 450  
Chicago, IL 60661

 312-654-0030

 [marketing@rkon.com](mailto:marketing@rkon.com)

## THE BACKGROUND

For over 75 years, our client has been a leading manufacturer of shelf-stable, dairy-based food and beverage products. Today, the company continues to grow as a top-tier source partner for food and beverage products, servicing large, fortune-500 companies nationwide.

## THE ASSESSMENT

In an instant, a \$200-million-dollar food company went from selling highly sought-after food products, to losing over \$1 million a day due to a single ransomware incident. It left all servers and endpoints exposed and at risk of losing key ingredients and data. To prevent further data loss, the company was forced to immediately shut down all production and operations, including infected servers, all networks, headquarters, and all facilities. The magnitude of this breach required a specialized partner to remedy.



## THE SOLUTION

The RKON incident response team wasted no time once brought in to search for the attack source and narrow down the possible vectors. Based on our in-depth analysis, we discovered the root cause of the ransomware attack was multifaceted, starting with an unsafe number of people using administrator accounts, misaligned leadership roles, incomplete backups, lack of documentation and patching schedules, and a nonexistent Disaster Recovery plan. Without consistent testing and a robust Disaster Recovery plan, the company was left at extreme risk for a breach.

While working with the data center provider, RKON immediately disabled all accounts, took over operational control, and thoroughly assessed the damage. To prevent further damage or risk, our incident response team worked 24/7, both onsite and offsite, in getting our client secure and back to production. RKON was able to quickly get the company back online by collaborating with C-suite executives to explain the breach, teaming with the IT department to remediate, and recommending security solutions to get the business live again and protect it from another detrimental breach in the future.

## THE OUTCOME

Our quick and effective recovery process saved more than just the company's critical systems; it saved the company's brand reputation as a trusted, reliable, and secure partner. RKON now plans to implement a Security Operations Center (SOC), Office365 migration, conduct holistic architecture reviews, and deploy ongoing vulnerability scans that will proactively safeguard information moving forward and strengthen security posture among all employees and vendors beyond just technology.

Don't let a ransomware attack almost put you out of business before taking security seriously. The best way to protect your most valuable assets is to invest in IT and partner with a team of experts who have the experience and truly understand what it takes to keep you safe.



**\$1 Million  
Saved per day**



**Onsite & Offsite  
Incident Response**



**Total Recovery  
Critical systems,  
reputation, & data**