Strauss Group Case Study

# How a Food Industry Leader Decreased Risk of Cyberattacks

## The Food Industry:
### Unique Vulnerabilities to Cyberattacks

According to US The Food Institute, a series of cyberattacks at high-profile food companies have sounded alarms throughout the industry over the last several years. Ransomware has become a frequent topic of discussion, leaving many businesses wondering—not if they will be attacked, but when? Dole, one of the largest produce companies in the world, was the most recent victim of a widely publicized cybersecurity incident that was identified as ransomware. The company released a statement addressing the attack after CNN reported that Dole had to temporarily halt production in North America and suspend shipments to grocers, citing a company memo.

"I think the food industry has unique vulnerabilities," said Brian Schnese, senior risk consultant at HUB International. Schnese, a former FBI Special Agent, explained that because the businesses in the food industry rely on a supply chain, cyberattacks can create a massive disruption.

## The Company:
### Strauss Group - One of the Largest Food Manufacturers in Israel

Strauss Group Ltd. is an Israeli manufacturer and marketer of consumer foods sold through retail stores. It is among the largest food manufacturers in Israel. Strauss Group focuses on dairy products, coffee, water, snacks, salads, and dips. Its subsidiary, Strauss Coffee, is a leading coffee company in Eastern Europe and Brazil. Strauss Group is a public company traded on the Tel Aviv Stock Exchange. Strauss Group has 15,000 employees worldwide and is active in more than 20 countries.

## The Challenge:
### Global Workforce, High Turnover


Most manufacturing companies experience high employee turnover. That challenge brings together employees with different cybersecurity training and knowledge backgrounds at any given time. Strauss Group also has a global workforce that works in six different native languages: Hebrew, Romanian, Polish, Serbian, Swiss-French, and Dutch. They were looking for a scalable solution that would allow the company to train its 5,000 users effectively.

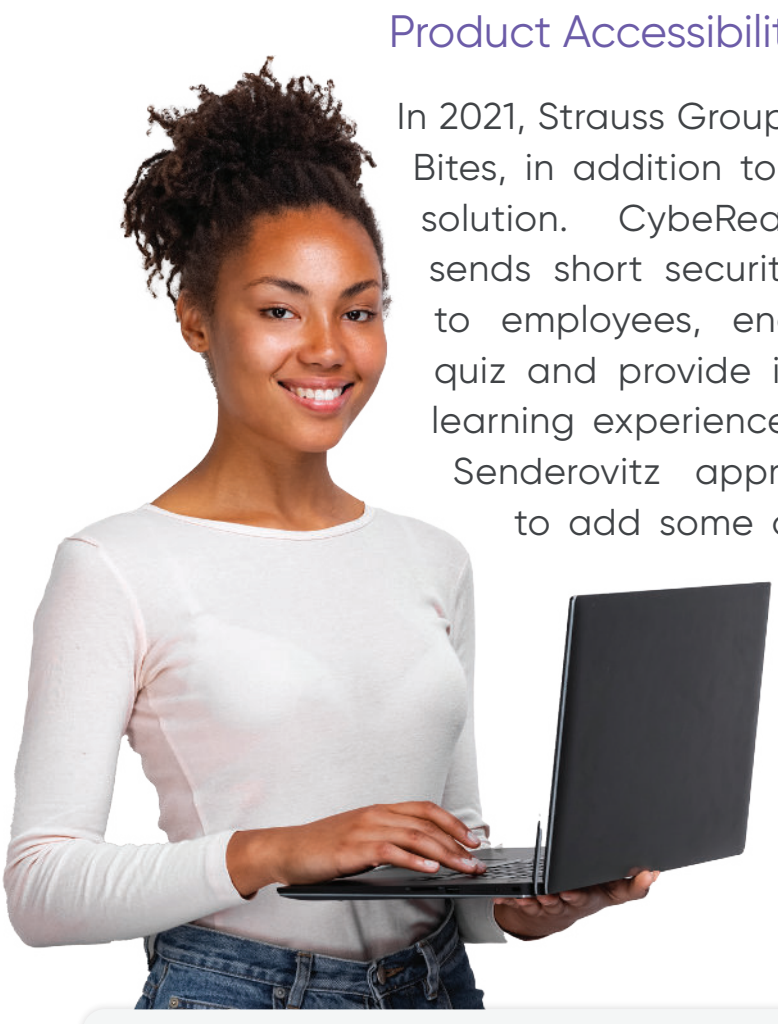

## The Solution:
### Out-of-the-Box Employees Readiness Program

In 2016, Strauss' global CISO Alon Senderovitz started evaluating a security awareness training solution that can help train the company's 5,000 users globally and reduce risk in light of the high turnover challenge.

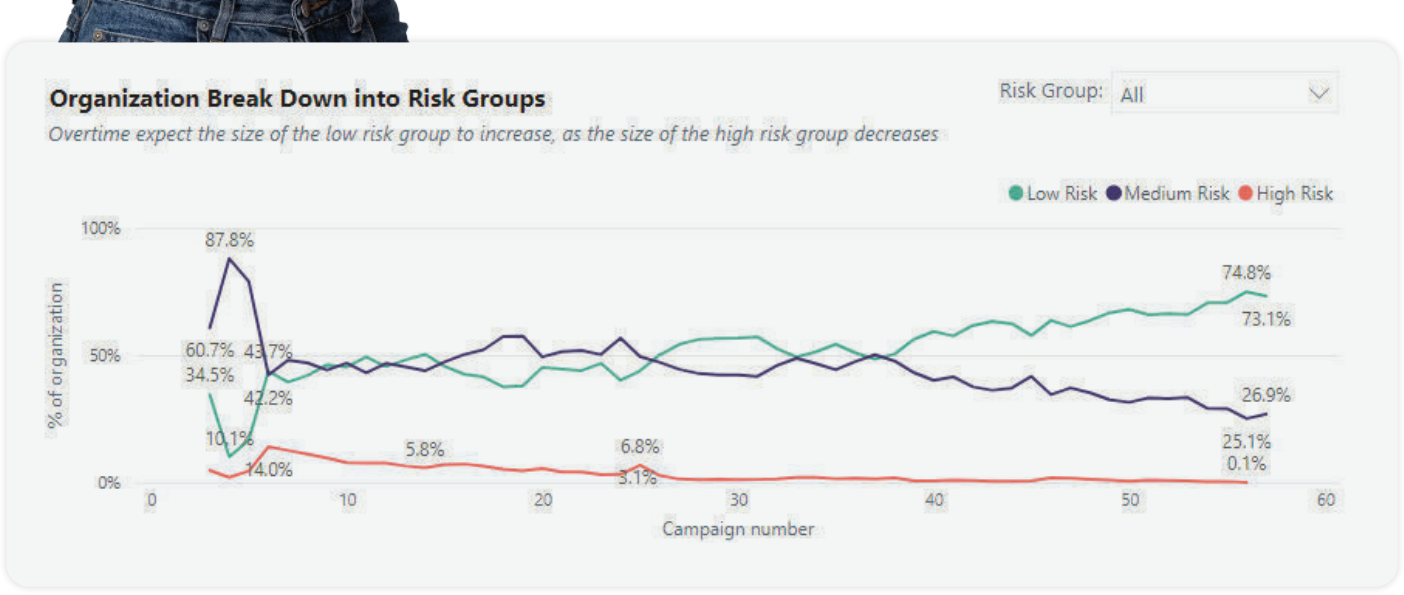
After comparing several security awareness training vendors, he chose CybeReady's solution for its potential to reduce risk without taxing the IT team. "CybeReady's solution is data-driven and has the adaptive capability to serve each employee short training sessions according to their risk group, seniority, role, and location," said Senderovitz. "We see new employees and high-risk employee groups train at double intensity until they can level up with the rest of their peers."

In addition to utilizing CybeReady's double-intensity training program for new and high-risk employees, Strauss used the Localization Engine to make the training more engaging for employees: "We train employees in their native language and locale (such as currency and other local attributes) automatically: this amazing know-how is all available out-of-the-box, and all we need to do is let the platform run the training."

### Product Accessibility



In 2021, Strauss Group started using CybeReady's Awareness Bites, in addition to the usage of the Phishing Simulation solution. CybeReady's Continuous Awareness Bites sends short security awareness content (micro sessions) to employees, encouraging them to answer a short quiz and provide immediate feedback to complete the learning experience. Shortly after deploying the solution, Senderovitz approached CybeReady and requested to add some accessibility add-ons to its Awareness training experience, so that the learning experience would be equally engaging for visually impaired employees. CybeReady's product team stepped up to the challenge, and within a couple of months, the accessible product became available to all CybeReady customers.




## The Results:
### From 12% to 0.1% Reduction in Employee High-Risk Group

When Strauss started using the CybeReady solution back in 2016, the high-risk group accounted for 12% of the organization. Within 12 months of training, the high-risk group decreased to 3%, and today it's as low as 0.1%.

In addition, the overall organization resilience Score to phishing has increased by about 5x within 12 months. Resilience Score is measured by the number of consecutive successes between two failed simulations. A higher Resilience score indicated that employees fall for phishing attacks less frequently.