

## Case Study

# How TBAuctions Auctioned Off Manual Processes and Dropped Their Phish-prone™ Percentage By 85% with KnowBe4

## TBAUCTIONS

### Industry

Technology/  
Software

### Headquarters

Amsterdam,  
Netherlands

### Challenge

Scaling security awareness and compliance with a small security team

Conversations about a circular economy are becoming more common, but TBAuctions is ahead of the curve. The B2B online auction platform has been enabling companies to sell used business goods through online auctions for almost a decade. The organization sources assets locally and sells them globally, serving industrial sectors such as transport and logistics, construction, agriculture and medical in more than 150 countries.

Supporting that global operation requires a strong approach to security and compliance. For Jasper van der Straten, a DevOps engineer at TBAuctions, managing these topics with a small security team meant finding a way to run security training, phishing tests and compliance initiatives at the right frequency without relying on time-intensive manual processes.

## At a Glance

- ▶ Security awareness scaled to colleagues throughout Europe
- ▶ Phish-prone™ Percentage reduced from 40% to 6%
- ▶ Hours of manual campaign work reduced to minutes

## Manual Efforts Limited Scalability

Working with so many entities meant security awareness and compliance had to be top of mind. It was — but it was also highly manual, leaving little bandwidth for anything else.

“We were basically creating material manually, sending out handcrafted company-wide phishing emails and creating newsletters,” van der Straten says. “This took quite some time, especially with our small team.”

This approach also made it difficult to meet the growing needs of the organization. As TBAuctions continued to scale internationally, van der Straten knew the existing approach wasn’t sustainable.

“Our previous approach wasn’t sufficient,” van der Straten says. “We could never have the proper frequency of high quality material we wanted to send out to the team.”

## Comprehensive Content and Enhanced Automation

The TBAuctions team began evaluating platforms that could support security awareness and compliance without adding a heavy operational burden. Ease of use, automation and content availability were key, along with the ability to support a multilingual workforce.

“After reviewing a couple of vendors, we found that KnowBe4 had a good track record,” van der Straten says. The large library impressed the team, featuring content that was:

- Customizable
- Built to address security awareness training and phishing tests
- Compliance-friendly
- Multilingual

KnowBe4 also integrated with Microsoft 365 and featured automated employee onboarding and offboarding workflows, making the platform an easy addition to TBAuctions’ existing security stack.

TBAuctions started with KnowBe4 [Security Awareness Training](#) and soon adopted [Compliance Plus](#) to remove the effort of drafting compliance material. Today, they run scheduled training campaigns, phishing tests and policy-based training without relying on manual content creation.

“Compliance Plus allows us to train people on the company policy rather than just sending it out and expecting people to read it,” van der Straten says.

They can even send out biweekly phishing tests if they feel it’s necessary. “That’s just not feasible if you’re working manually,” van der Straten adds.

Another benefit? Automation — namely AI Defense Agents (AIDA)™. AIDA automates training and phishing simulations based on user profiles and security maturity. It identifies and addresses awareness gaps of individual users, creating a highly personalized program that doesn’t require any additional effort from the security team.

“Automation was key. Tailoring training isn’t something we could do ourselves, even with a bigger team,” van der Straten says. “You can just set up a campaign and the AI Defense Agents will basically do the rest.”

## Reducing Phish-prone™ Percentage by 85%

Since implementing KnowBe4, TBAuctions has seen a measurable reduction in human risk. The company’s phishing test performance was a clear indicator of progress: “Our initial Phish-prone™ Percentage was around 40%,” van der Straten says. “After a couple of phishing training sessions, that dropped a lot. We’re currently at 6%.”

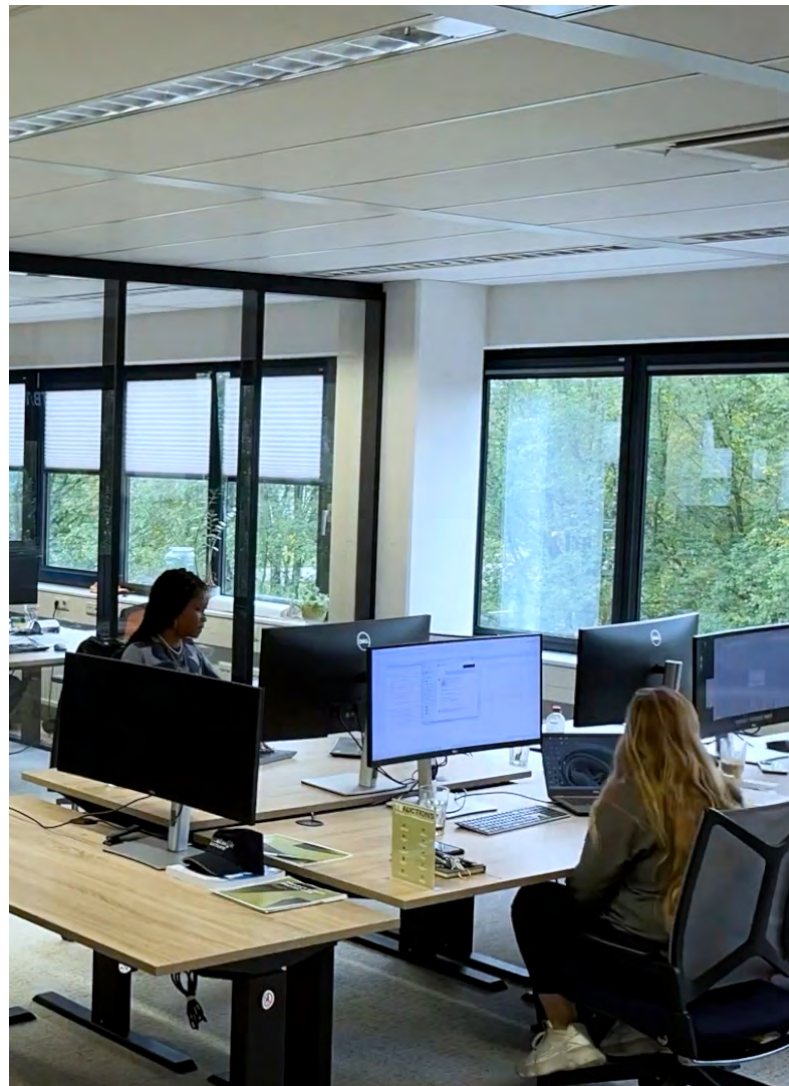
Beyond the numbers, van der Straten and his team notice a change in how employees engage with security on a day-to-day basis. Employees are more involved and more cautious when interacting with email and links.

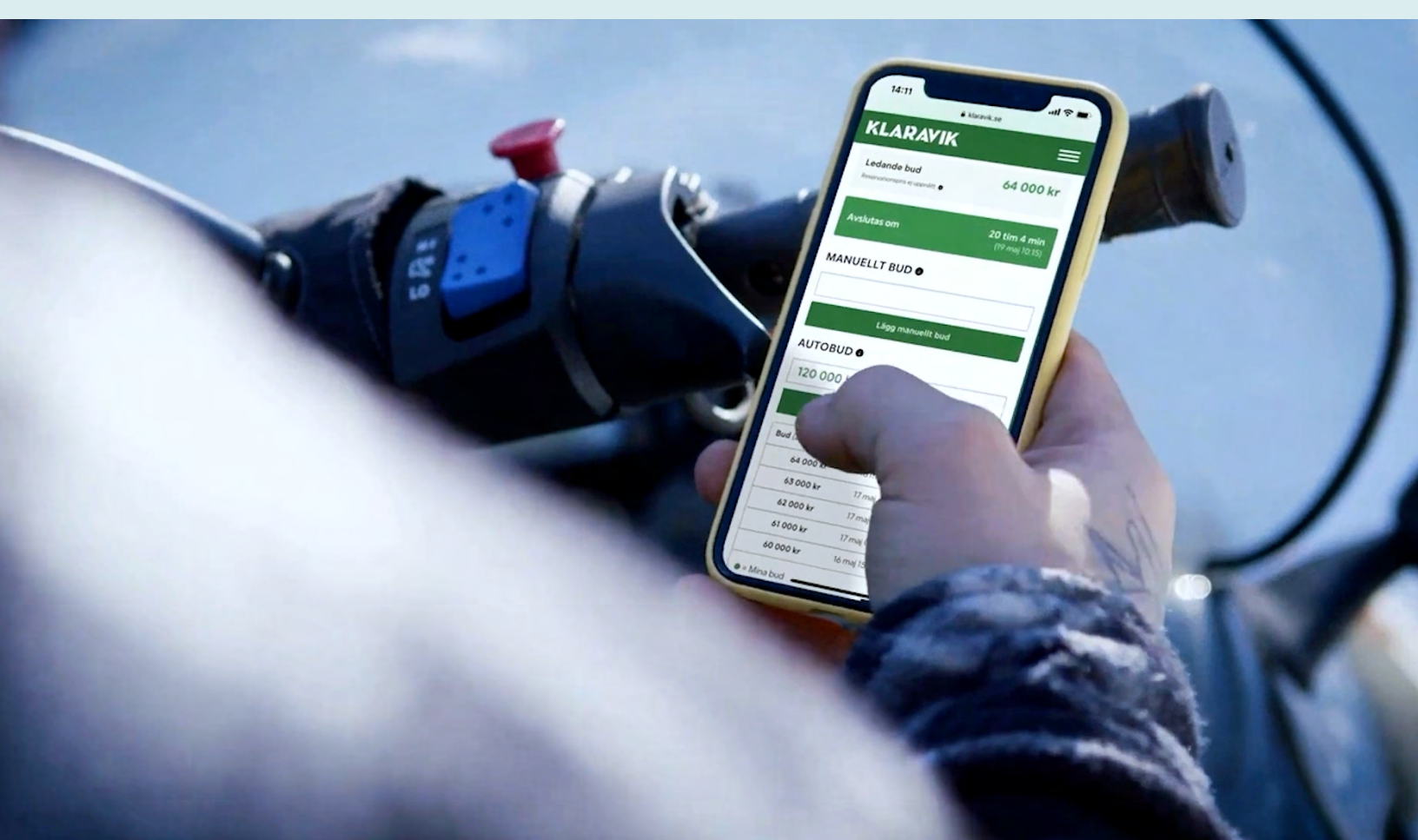
“We see that in the amount of reported phishing emails, be it tests or real-life examples,” van der Straten says. “They’re calling up the help desk way more often, asking if a certain email is real or if they can click a certain URL, rather than doing that and having us pick up the pieces afterwards.”

The shift has reduced the operational burden for TBAuctions’ small security team. Tasks that previously required hours now take a fraction of the time. “Before, a phishing campaign would take several hours of setup,” van der Straten says. “Now it’s done in a matter of clicks. That’s hours versus minutes.”

*“Our initial Phish-prone™ Percentage was around 40%. After a couple of phishing training sessions, that dropped a lot. We’re currently at 6%.”*

*—Jasper van der Straten, DevOps engineer, TBAuctions*





## Ongoing Awareness Key to a Strong Security Culture

For organizations with small security teams, van der Straten believes that balance between strong security awareness and operational feasibility is critical. KnowBe4 helps them maintain that balance.

“If we don’t use KnowBe4, I know that the frequency and the quality of the training and phishing tests will drop,” van der Straten says.

He also points to the ongoing value of having up-to-date content readily available: “KnowBe4 content gets refreshed all the time. That saves a lot of work you would otherwise have to do yourself.”

The increased efficiency gives van der Straten’s team more time to focus on strategic risk decisions rather than operational tasks. It also means they can consistently reinforce security awareness at the frequency required to keep up with emerging threats. The company’s growing workforce is smarter, savvier and better protected than before, and that’s due in large part to KnowBe4.

0326-US



KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755  
855-KNOWBE4 (566-9234) | [www.KnowBe4.com](http://www.KnowBe4.com) | [Sales@KnowBe4.com](mailto:Sales@KnowBe4.com)

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.