Case Study

CoreDux Builds a Stronger Human Defense with KnowBe4

COREDUX®

Industry

Manufacturing

Location

Netherlands

Challenge

Improve user phishing awareness and resilience amid increasing regulatory pressure, supply-chain requirements, and evolving threats, without overburdening a small IT team.

CoreDux is a Netherlands-based, all-in-one product and technology company. It develops original design manufactured (ODM) products, manufactures micro precision components and enables integrated solutions for highly regulated and security-sensitive environments, including various high tech clients that are critical suppliers to the global semiconductor industry.

With approximately 500 employees across the Netherlands, France and the U.S., CoreDux faces the challenge shared by many growing industrial organizations: how to build a consistent security culture across a diverse workforce with varying levels of digital exposure.

For Deen van Rijn, Director of IT at CoreDux, the answer was clear. Technical controls alone were not enough.

“You can have 10 locks on your door, but if people leave it open, the locks don’t matter,” van Rijn says. “User awareness had to become part of our defense-in-depth cybersecurity strategy.”

At a Glance

- Phish-prone™ Percentage reduced from ~12% to a 5% average, with 2% in recent campaigns
- 900 suspicious emails reported in six months via the KnowBe4 Phish Alert Button, improving early detection
- Faster campaign creation and easier reporting compared to previous platform
- Stronger security culture, with increased user engagement and reduced human risk

A Proactive Shift Driven by Regulation and Risk

As a European organization subject to NIS2 requirements and operating within ASML's critical ecosystem, van Rijn understood the contribution that security awareness training could make to the company's overall security posture.

"CoreDux did not adopt security awareness training in response to an incident. Rather, cybersecurity is getting more complex, and regulation is raising the bar, so it became clear that adding a robust human layer to our cyber programs was not only responsible, but practical," van Rijn says.

Before selecting KnowBe4, CoreDux was using a competing platform for training and phishing simulations. The experience fell short. Customization was limited, reporting was clunky, and the overall workflow made it hard for the IT team to operate efficiently.

In a highly dynamic environment, ease of deployment and automation were critical factors in evaluating alternatives.

> *"You can have 10 locks on your door, but if people leave it open, the locks don't matter. User awareness had to become part of our defense-in-depth cybersecurity strategy."*
>
> Deen van Rijn, Director of IT, CoreDux

Why CoreDux Chose KnowBe4

After evaluating options, CoreDux selected KnowBe4 Security Awareness Training for its ability to combine phishing simulations, training and reporting into a single, easy-to-manage platform.

"What stood out about KnowBe4 was how quickly we could get value," van Rijn says. "You can build a full phishing campaign with real variation in just minutes, instead of spending days or weeks configuring it."

CoreDux initially rolled out KnowBe4 to approximately 300 users across its Netherlands and France locations, covering nearly all employees with corporate email accounts. Built-in language support played a key role in adoption, particularly for French employees.

"If we wanted realistic results, people needed to receive messages in their own language," van Rijn says.

Establishing a Structured Program to Arm Employees to Spot Threats

With KnowBe4, CoreDux implemented a structured program that balances effectiveness with operational impact:

- Biweekly simulated phishing emails sent to users
- Quarterly training assignments, with three modules selected per cycle
- Mandatory remedial training for repeat clickers
- Strong emphasis on using the Phish Alert Button (PAB), which is built into CoreDux's email client, to flag suspicious emails directly to van Rijn's team

The goal was not just to reduce clicks, but to encourage active participation in identifying potential threats.

"We don't want people to just delete suspicious emails," van Rijn says. "We want them to report them so my team can act quickly if something real gets through. The Phish Alert Button makes that simple and seamless."

> *"We don't want people to just delete suspicious emails. We want them to report them so my team can act quickly if something real gets through. The Phish Alert Button makes that simple and seamless."*
>
> Deen van Rijn, Director of IT, CoreDux

> *"People are clicking less, and they're thinking more critically about what lands in their inboxes. This alone makes KnowBe4 a valuable asset."*
>
> Deen van Rijn, Director of IT, CoreDux

Measurable Improvements in Human Risk

The results were immediate and measurable. When CoreDux began phishing simulations, the organization's Phish-prone™ Percentage (PPP) was approximately 12 percent. As the program matured and simulations became more sophisticated, results improved significantly. The company's current PPP is at 5% but it has been as low as 2%. These results are dramatically below the manufacturing industry benchmark of 21 percent.

"These numbers tell us two things," van Rijn says. "People are clicking less, and they're thinking more critically about what lands in their inbox. This alone makes KnowBe4 a valuable asset."

At the same time, reporting behavior has increased. Over a six-month period, CoreDux employees reported approximately 900 suspicious emails using the PAB.

"Reporting through the PAB doesn't save us time in the short term, but it absolutely reduces risk, which is our main goal," says van Rijn. "If one real email gets through and someone reports it through the PAB, that's KnowBe4 doing exactly what it's supposed to do."

Building a Security-Conscious Culture

Beyond metrics, van Rijn has seen a cultural shift across the organization. Employees openly discuss phishing simulations, compare experiences and demonstrate a higher level of skepticism toward unexpected messages.

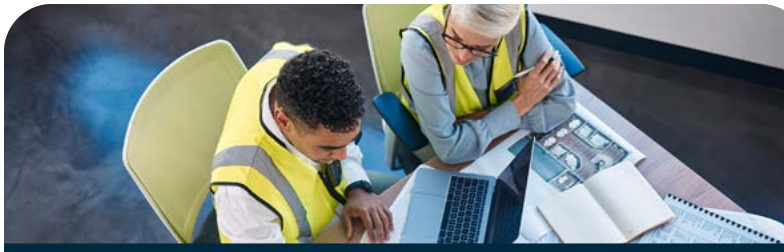
"When people stop me in the hallway to tell me they spotted a phishing email, that's a win. Even when internal newsletters get reported, it shows people are aware and thinking critically," says van Rijn.

Security awareness has also gained visibility at the leadership level. Cybersecurity metrics are reviewed as part of IT steering committee discussions, reinforcing the idea that human risk is a business issue, not just a technical one.

Looking Ahead

CoreDux plans to expand its KnowBe4 program in 2026 by introducing mandatory training policies and increasing physical awareness initiatives. The company has recently purchased KnowBe4 Defend and Prevent modules and has extended the complete platform to CoreDux USA, as well.

"We're still maturing, but we've built a strong foundation, and KnowBe4 gives us the flexibility to keep improving without adding complexity," van Rijn says.



"We're still maturing, but we've built a strong foundation and KnowBe4 gives us the flexibility to keep improving without adding complexity."

Deen van Rijn, Director of IT, CoreDux

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