



CYBERDISE

Based on the latest scientific findings on AI and human behavior

Another CYBERDISE solution – implemented at:



GLB Group – Building a Sustainable Security Culture with CYBERDISE Awareness



AT A GLANCE

Industry

Construction company.

Challenge

Protecting craftworkers, construction teams, systems, and data from the risks posed by cybercriminals.

Solution

- CYBERDISE Business Edition.
- Regular training tailored to the work context and phishing campaigns.

Advantages

- A simple and intuitive solution from CYBERDISE.
- Compatible with existing IT infrastructure.
- LMS can be used for third-party courses.
- AI simplifies operations.
- Wide range of customization options within the CYBERDISE software.
- Stronger protection through better-informed employees, evident by measurable awareness gains.

The GLB Group

The GLB Group, headquartered in Langnau in the Emmental region, is a leading provider of construction, timber construction, and real estate services in Switzerland. Bringing together craftsmanship, planning expertise, and modern construction execution under one roof, GLB serves both private and commercial clients through a network of locations and over 1,100 employees. The group is known for its strong regional roots, commitment to quality, and focus on sustainability.

CHALLENGE

"We've implemented extensive IT security measures at GLB Group - firewalls, rapid patching, endpoint protection, and more - yet people remain the primary entry point for cyberattacks," says Ismael Aemisegger, Head of IT Support at GLB Group.

According to a 2024 IBM study, over 47% of successful cyberattacks originated from employee actions. At the same time, the average financial damage has increased by

20% over the past five years, reaching \$4.88 million.

A particular challenge for GLB: the workforce primarily consists of skilled tradespeople who don't work at a computer regularly. Traditional phishing simulations - designed for office-based service companies - fall short in this context. They target employees with daily email use, which does not reflect the typical work environment on a construction site.

SOLUTION

GLB Group recognized this challenge early on. "To continuously train our employees and strengthen their security awareness, we rely on CYBERDISE Awareness," says Ismael Aemisegger.

CYBERDISE platform enables GLB to run a tailored awareness program. This includes targeted, partially customized training sessions, localized phishing simulations of varying difficulty levels, and of course, a structured evaluation of the results. CYBERDISE Awareness has also been integrated with



"What's truly impressive is the increased level of awareness achieved through AI. GLB employees who were exposed to AI-personalized phishing simulations showed over 50% higher awareness in follow-up assessments."

"The growing threat landscape from targeted attacks reinforces our commitment to investing in our employees' security awareness," says Ismael Aemisegger.

With this approach, GLB Group is well on its way to establishing a strong, lived security culture within the organization - providing lasting protection against cyber risks.

Microsoft Azure Apps and Active Directory. In addition, the internal team received thorough product training.

BENEFITS

GLB was particularly impressed by the intuitive usability of the CYBERDISE solution. Thanks to its customizable features and the ability to localize templates, campaigns could be launched quickly and effectively.

A wide range of learning modules - from interactive courses and videos to simulations - enables varied and hands-on learning experiences.

Furthermore, CYBERDISE Awareness is built with the highest standards of data protection and security in mind. The solution is fully compliant with Swiss and EU data protection regulations (DSG / GDPR), offers strong encryption at both the application and database levels, and uses anonymized data collection by default - all without compromising individual aware-

ness scoring.

RESULTS

"The initial results clearly demonstrated the effectiveness of our measures: employees who were exposed to simulated phishing emails noticeably changed their behavior. Awareness of IT security has significantly increased," summarizes Ismael Aemisegger.

The impact became evident through a steady rise in employee attentiveness and sensitivity to security risks. Particularly effective were the realistic and, above all, AI-generated phishing campaigns.

Internal analyses confirm that CYBERDISE awareness programs significantly enhance a company's overall security posture. This was quickly apparent at GLB - a clear testament to the platform's effectiveness.



[cyberdise-awareness.com /download](https://cyberdise-awareness.com/download)

Cyberdise AG, Poststrasse 26, CH-6300 Zug, Switzerland, +41 44 551 78 10
backoffice@cyberdise.io | support@cyberdise.io