

RAIL FREIGHT / CRITICAL INFRASTRUCTURE · CYBERSECURITY AWARENESS · MANAGED AWARENESS TRAINING (M/AT)

From Microsoft Workarounds to a Measurable Risk Program: Governing Human Risk Across a Multi-Country Rail Operation

How Banyax replaces a limited Microsoft phishing module with a fully managed awareness program — delivering executive-level KRI reporting, multi-country simulation coordination, and measurable human risk reduction.

INDUSTRY Rail Freight / Critical Infrastructure · Mexico + USA · Multi-Country Operation

01 · RESULTS AT A GLANCE

Four outcomes that demonstrate what a managed awareness program delivers that a Microsoft module never could.

<p>Prior State</p> <p>Workaround</p> <p><i>Microsoft module — limited scope, no simulation</i></p>	<p>Coverage</p> <p>Multi-country</p> <p><i>coordinated across Mexico and US-based teams</i></p>	<p>Renewals</p> <p>1 completed</p> <p><i>renewed with no identified risk to retention</i></p>	<p>Referrals</p> <p>2 generated</p> <p><i>Florida East Coast + GCC — active word-of-mouth</i></p>
--	---	---	---

Before Banyax, the organization ran its security awareness program entirely in-house using Microsoft's phishing simulation module. Simulations were limited in scope, could not reach all users, cover few training topics, and generated no meaningful risk metrics. Program administration was manual and time-consuming for the internal IT team.

After Banyax, the organization has a fully managed awareness program delivering executive-level risk reporting, multi-country coordinated simulations, and measurable KRI trends. Leadership now receives a quantified view of human risk — and the program has already generated two external referrals to affiliated organizations.

02 · THE BUSINESS PROBLEM

The organization recognized that its existing approach to security awareness was generating activity but not visibility. Simulations were partial, very basic, and easy-to-guess phishing templates for a general public; training content was thin, and there were no metrics that leadership could use to understand the organization's actual human risk exposure.

<p>Microsoft workaround, not a program</p> <p>The organization used Microsoft's phishing simulation module as its primary tool. Simulations had limited personalization, couldn't target all users, offered few training modules, and required significant manual effort to administer — from simulation design to internal communications.</p>	<p>No risk metrics for leadership</p> <p>The security team had no quantified baseline of the organization's phishing susceptibility. There were no KRIs, no trend data, and no way to present human risk to senior leadership in measurable, comparable terms that improve over time.</p>	<p>Multi-country coordination gap</p> <p>With operations spanning Mexico and connections into the United States, the organization needed a program that could coordinate awareness activity across different geographies, time zones, and team structures — something a single-country, single-tool approach could not deliver.</p>
--	--	--

03 · WHAT BANYAX BUILT — MANAGED PROGRAM, NOT A MODULE

Banyax replaced a manual, limited Microsoft module with a fully managed awareness program: targeted phishing simulations for all users using complex levels of difficulty, executive-level risk reporting, cross-country coordination, and a structured training content library through KnowBe4.

<p>Executive-level risk reporting</p> <p>Banyax conducted executive presentations for each simulation exercise, giving leadership visibility into phishing susceptibility rates, highest-risk departments, and training completion trends. For the first time, the Chief Information Security Officer (CISO) could present human risk as a board-level Key Risk Indicator (KRI), not a technical summary.</p> <p>Differentiator: <i>Translating simulation data into executive risk reporting is what separates a managed program from a tool. Banyax built the narrative and the metrics together.</i></p>	<p>Multi-country coordination & KnowBe4 depth</p> <p>Simulations and training activities were coordinated across teams in Mexico and the United States, with aligned communication strategies and consistent reporting across geographies. Banyax managed the complexity of cross-border program execution that the internal team could not sustain alone.</p> <p>Vertical context: <i>Rail freight operators have cross-border operational dependencies. A phishing attack that compromises a user on either side of the border can have supply chain implications on both. The program was designed with that risk profile in mind.</i></p>
---	---

KnowBe4 content library — depth that Microsoft can't match

The client specifically valued the breadth and quality of KnowBe4's training content. The library covers topics and scenarios that a generic Microsoft module does not — and is updated continuously to reflect current threat patterns. That depth is part of what drives renewal and referral behavior in this client.

04 · OUTCOMES — BEFORE AND AFTER

Before

Partial phishing simulations via Microsoft module. No full-organization coverage. Limited training content. No executive risk reporting. Manual administration consuming 1–2 IT team members. No cross-country coordination capability.

The referral story

This client recommended Banyax to two organizations: a U.S.-based rail operator with cross-border operational ties, and a corporate group dedicated to the manufacturing of cement and other construction materials in northern Mexico. Both referrals were unsolicited — the client recommended the program based on results, not incentives.

After

Full-organization simulation program. Executive presentations with KRI metrics. Multi-country coordination active. Internal IT team freed from manual administration. Program renewed. Two referrals generated to external organizations.

Expansion pipeline

The client has expressed interest in expanding its cybersecurity strategy to leverage additional Banyax capabilities beyond Managed Awareness Training (M/AT). The awareness program is the foundation of a broader engagement that the client is driving.

INVESTOR SIGNALS

Retention Renewed — 1 completed renewal

Referrals 2 active

Expansion Client actively seeking broader engagement

Geography Mexico + USA cross-border program active

Efficiency 1–2 IT FTEs freed from manual administration

“For the first time, we could show leadership a quantified view of where our human risk actually was — not a training completion rate, but a real susceptibility metric that moves over time.”

— Information Security Lead, Major Mexican Rail Freight Operator

The expansion interest confirms what the referrals already showed: this is a client that has moved from satisfaction to invested.

05 · IDEAL CLIENT PROFILE

Rail freight operators, logistics companies, and critical infrastructure organizations with geographically distributed workforces spanning multiple countries — particularly those relying on Microsoft tools as a workaround for security awareness, with no quantified KRI for human risk, or where a phishing compromise could trigger cross-border operational or supply chain disruption.

06 · LEARN MORE & CONTACT

Learn more about Banyax M/AT

Discover how Banyax's Managed Awareness Training (M/AT) service transforms passive security awareness modules into a measurable human risk governance program — with KnowBe4-powered simulations, executive-level KRI reporting, and coordinated multi-country execution.

Visit: banyax.com

Want to learn more?

If this document was forwarded to you and you'd like to explore how Banyax can help your organization govern human risk — reach out directly.

Email: marketing@banyax.com

Website: banyax.com