AVIATION · CYBERSECURITY AWARENESS · MANAGED AWARENESS TRAINING (M/AT) · MANAGED EXTENDED DETECTION & RESPONSE (M/XDR)

When a High-Level Employee Clicks the Link:

Building a Security Culture That Starts at the Top

How Banyax transformed a passive SuccessFactors awareness module into a measurable human risk governance program — where the CEO personally experienced a phishing simulation and the security conversation reached board level.

INDUSTRY Aviation / Passenger Air Transport (Low-Cost Carrier) · Mexico

01 · RESULTS AT A GLANCE

Four outcomes that changed how the airline measures and governs human risk — the most unpredictable attack surface in any organization.

Starting Point	Visibility	Board Signal	IT Efficiency
Zero	**Full org**	**CEO**	**1–2 FTE**
no phishing simulation capability before Banyax	*100% of employees now covered and measurable*	*executive leadership personally experienced a simulation*	*internal team hours freed from manual awareness management*

Before Banyax, the airline's security awareness program consisted of limited modules loaded into SuccessFactors. There were no phishing simulations, no structured internal communications on security topics, and no way to measure the organization's actual susceptibility to social engineering attacks.

After Banyax, the organization has full visibility into human risk across its workforce: measurable phishing susceptibility rates, structured training cadences, and executive-level reporting on awareness KRIs. The security team knows exactly where its exposure is — and can show the board a trend, not just an incident.

02 · THE BUSINESS PROBLEM

Phishing is the leading initial access vector in aviation. The airline knew this — because it had seen it happen to affiliated carriers in the same group. What it lacked was a program capable of measuring, training, and governing human risk at the scale and sophistication the threat required.

No simulation capability

The airline's SuccessFactors platform provided passive awareness content but no phishing simulations. Without simulations, there was no way to know which employees were susceptible, which departments were highest risk, or whether the program was working at all.

No risk visibility for leadership

Management had no quantified view of human risk. Security reports were narrative, not metric-driven. There was no KRI for phishing susceptibility, no trend data to show the board, and no way to connect training investment to measurable risk reduction.

Group-level context made urgency real

The risk was not theoretical. Affiliated airlines within the same group had experienced high-severity phishing attacks. The airline was operating without simulation or measurement capabilities while the threat environment around it was already active.

03 · WHAT BANYAX BUILT — FROM PASSIVE MODULES TO ACTIVE PROGRAM

Banyax replaced passive content delivery with a structured, measurable security awareness program: phishing simulations tailored to the airline's operational context, executive-level reporting on risk metrics, and a training cadence designed for a large, distributed workforce.

The simulation that changed the conversation

During a phishing simulation exercise, the CEO clicked the link. That single event — the organization's most senior leader personally experiencing what a successful phishing attempt feels like — generated an internal conversation about security culture that no training deck could have triggered. It demonstrated, at the highest level of the organization, that susceptibility to social engineering is not a junior employee problem. It is a leadership problem. And measuring it is the only way to govern it.

Phishing simulations at scale

Targeted phishing simulations deployed across the full employee base — not limited to a sample. Scenarios tailored to the airline's operational context: communications that look like internal HR, operations, or IT messages employees receive regularly.

Vertical context: *Aviation employees receive high volumes of operational communications. Banyax designed simulations that mirror the specific language and format of messages employees are conditioned to trust.*

Executive reporting & Managed Awareness Training (M/AT) + Managed Extended Detection & Response (M/XDR) integration

Banyax conducted webinar-format sessions for the airline's leadership team, presenting simulation results, susceptibility trends by department, and recommended actions. Security risk was presented as a measurable organizational KRI — not a technical report.

M/AT + M/XDR integration: *The airline already had Managed Extended Detection & Response (M/XDR) active. M/AT adds the human layer: when a simulated phishing attempt is clicked, the Security Operations Center (SOC) has context. When a real phishing attempt is detected externally by M/XDR, the awareness program is updated to reflect the actual threat pattern.*

04 · OUTCOMES — BEFORE AND AFTER

Before

Passive awareness modules in SuccessFactors. No phishing simulations. No visibility into susceptibility rates. No executive reporting on human risk. Security team managing content manually with 1–2 IT members dedicated to administration.

Challenges and maturity

The early stages of the engagement required a higher level of technical accompaniment to get the program fully operational. That ramp-up period is now behind the client. The program is mature, stable, and delivering consistent results — a natural part of standing up a structured awareness function where none existed before.

After

Full-organization phishing simulation program. Measurable susceptibility KRIs reported to leadership. Executive team directly engaged — including the CEO. Internal IT team freed from manual administration. Security culture conversation elevated to board level.

Group-level opportunity

The client belongs to an aviation group where affiliated carriers have already experienced phishing attacks. The M/AT program architecture Banyax built is designed to scale across multiple entities — making this a natural expansion candidate for group-wide deployment.

INVESTOR SIGNALS

Retention Active — first renewal imminent, no risk identified

Stack depth M/XDR + M/AT — two services, one client

Group upside Multi-carrier group — natural expansion path

Board signal CEO engaged directly in simulation exercise

Efficiency 1–2 IT FTEs freed from manual administration

"When the CEO is the one who clicks the link, the conversation about security culture changes at every level of the organization."

— Information Security Lead, Major Mexican Low-Cost Airline

And with affiliated carriers in the same group already hit by phishing attacks, the cost of not having this program is visible and recent.

05 · IDEAL CLIENT PROFILE

Airlines, aviation groups, and large-workforce organizations where phishing is a known and active threat — particularly those with affiliated entities that have experienced incidents, with passive awareness programs that generate no measurable KRI, or operating at a scale where 100% employee coverage and executive-level susceptibility reporting would shift the security conversation from IT compliance to business governance.

06 · LEARN MORE & CONTACT

Learn more about Banyax M/AT (Managed Awareness Training) + M/XDR (Managed Extended Detection & Response)

Discover how Banyax's M/AT and M/XDR work together to measure, train, and govern human risk — turning a passive awareness module into a board-level security governance program.

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