CYBERREADY

From Legacy Awareness to Cyber Readiness:

How to Build Employee Instincts at Any Scale

May 2026

Agenda

- Introducing our speakers
- The old awareness model is becoming less relevant
- What modern readiness needs to do today
- From theory to proof
- What leaders should stop accepting from old programs
- Q&A

CYBERREADY

Introducing

Ing. Daniel ČEP

IT-Governance (FIG) | IT Security | LISO

ŠKODA

CYBERREADY

Introducing

Noam Brosh

IT Security
Chief Information Security Officer

CYBEREADY

Awareness Was Built
for Yesterday's Threats

- Security teams added more tools
- Threats became faster, personalized, and deceptive
- Employees are a larger and dynamic part of the attack surface

Training completion

Being better prepared

What changed in the real world that made the old training model feel **less relevant?**

- Long and boring E-learning courses.
- Employees not reading. Need to memorize everything.
- Users are multitasking. Impossible to keep their attention.
- Real experience, not just theory –"I would never click on that.“

If awareness is no longer enough, what should a modern program delivered today vs. 10 years ago?

- Move from knowledge to instinct
- Match today's real attack patterns
- Prove behavior change, not completion
- Adapt to each employee automatically
- Reduce workload for the security team
- Fit fast-moving organizations
- Deliver continuous, targeted micro-learning

Why does **“training-delivered”** no longer mean **“readiness-achieved”**?

- Completion rates can hide real risk
- Phishing incidents can rise even when training is “done.”
- The old model was built for a slower work environment
- Employees now work across cloud apps, Slack, email, and constantly switch context
- Attackers now weaponize real-time events and local news
- Training must match the speed of the business
- If it does not reduce risk, it is only checking a box

What becomes non-negotiable if you want the program to work in real life, not just in theory?”

- Continuity
- Delivering fresh & up-to-date content
- Onboarding and training new employees
- Operational simplicity
- Realistic expectations for progress
- The program evolves — Smishing, Security Bites, Teams

What Real Employee Progression Looks Like
When Readiness Is Working?

- Different people - different behaviour
- Improvement over time
- Never expect 100% resilience
- Don‘t let users fall asleep
- Users:

  - Different devices

  - Delegations for email access
- Training blockers – other security technologies

How to Know Training Is

Changing Behavior

- ✓ Look past 100% completion reports
- ✓ Measure behavior under real work pressure
- ✓ Training must fit into the employee’s workflow
- ✓ Fast-moving teams need zero-friction learning
- ✓ Track resilience trends, not quiz scores
- ✓ Use short learning moments when risk appears
- ✓ Real progress means employees pause before they click

What Should Security Leaders Stop Settling For?

- Stop accepting heavy admin work
- Stop relying on once-a-year training
- Stop measuring completion as success
- Demand autonomous program management
- Demand learning that adapts to behavior
- Demand short training moments in real time
- Demand resilience metrics that prove readiness

What Should Mature Teams Demand from a Program Built to Scale?

- Continuous support from Customer Success
- Automation and operational simplicity
- Delivering fresh and engaging content
- Supporting onboarding and training of new employees
- The program continuously evolves and improves over time
- Long-term process with realistic expectations and measurable progress

CYBERREADY

Q&A

Ready to Move from Awareness to Readiness?

Choose an engaging, relevant, and fully automated cybersecurity training program that transforms employees into a proactive line of defense while freeing CISOs and security teams from endless manual work

asaf@cybeready.com

CYBEREADY