DEATH BY COMPLIANCE: WHAT MANDATORY SECURITY TRAINING ACTUALLY TEACHES YOUR EMPLOYEES

Daniels Heincis

BSides Riga 2026

A B O U T M E

- Cybersecurity educator
- 7 years providing diferent kinds of education trainings/talks
- 5 years in cybersecurity
- Mārtiņa-CTF organizer
- Fun fact: this presentation took me around 48h to make but most of the slides were made in last 12h hours before presenting

SO WE ARE HERE AT BSIDES RIGA

Bside: Desktop Mate

Community Hub

In Bside, you create your original character Biibit, a living virtual buddy who finds a home on your desktop. Each Biibit grows, learns, makes friends, and develop its own unique view of the world. Together, Biibits create a cozy and vibrant world full of life, stories, and connections!

ALL REVIEWS:	Mostly Positive (37)
RELEASE DATE:	28 Oct, 2025
DEVELOPER:	BIIBIT
PUBLISHER:	BIIBIT

Popular user-defined tags for this product:

Early Access | Singleplayer | Casual | Character Customization | +

Bside: Desktop Mate

Community Hub

In Bside, you create your original character Biibit, a living virtual buddy who finds a home on your desktop. Each Biibit grows, learns, makes friends, and develop its own unique view of the world. Together, Biibits create a cozy and vibrant world full of life, stories, and connections!

ALL REVIEWS:	Mostly Positive (37)
RELEASE DATE:	28 Oct, 2025
DEVELOPER:	BIIBIT
PUBLISHER:	BIIBIT

Popular user-defined tags for this product:

Early Access | Singleplayer | Casual | Character Customization | +

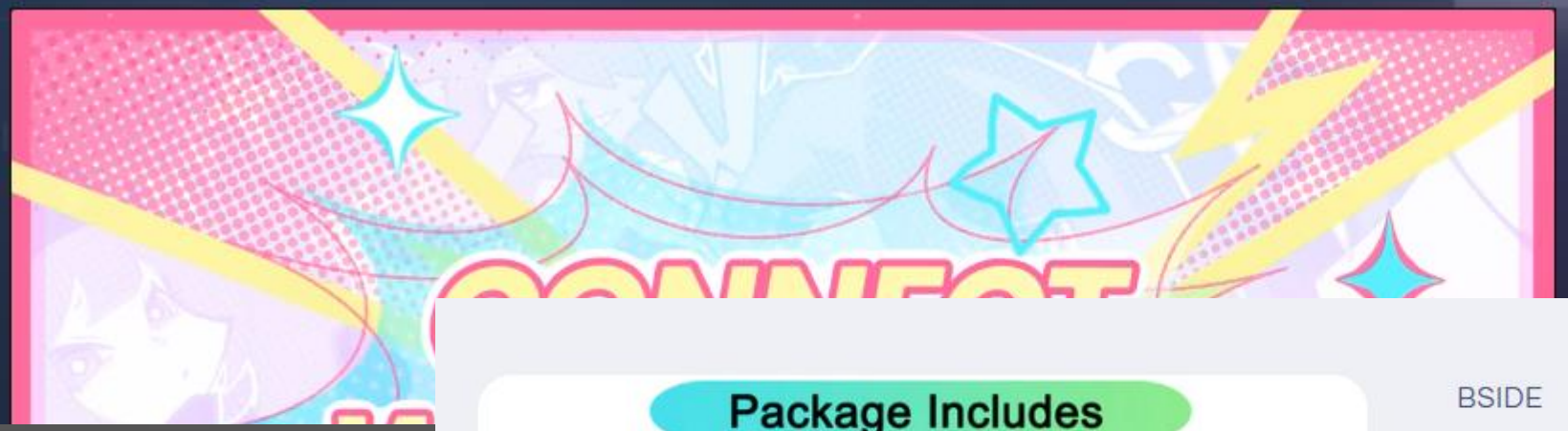
Bside

11 292 klausītāji mēnesī

Sekot

Bside: Desktop Mate

Community Hub



BSIDE

BSIDE S9LN New Digital Multimeter Smart 9999 DC/AC Voltage Tester Capacitance Resistance Diode NCV HZ Live Wire Detection Test

$18.80

Tax included.

SO WE ARE HERE AT BSIDES RIGA

21 seconds

Median time to click a phishing link

Verizon DBIR 2024

Once a year

Most common training cadence

Hornetsecurity 2024

71%

Say cybersecurity is a high priority

74%

Have no training programm

Flash Eurobarometer 547, EU-27, 2024

93%

Apply at least one security measure

60%

Train staff at all

Eurostat 2024

2x

EU median security spending

Doubled in one year

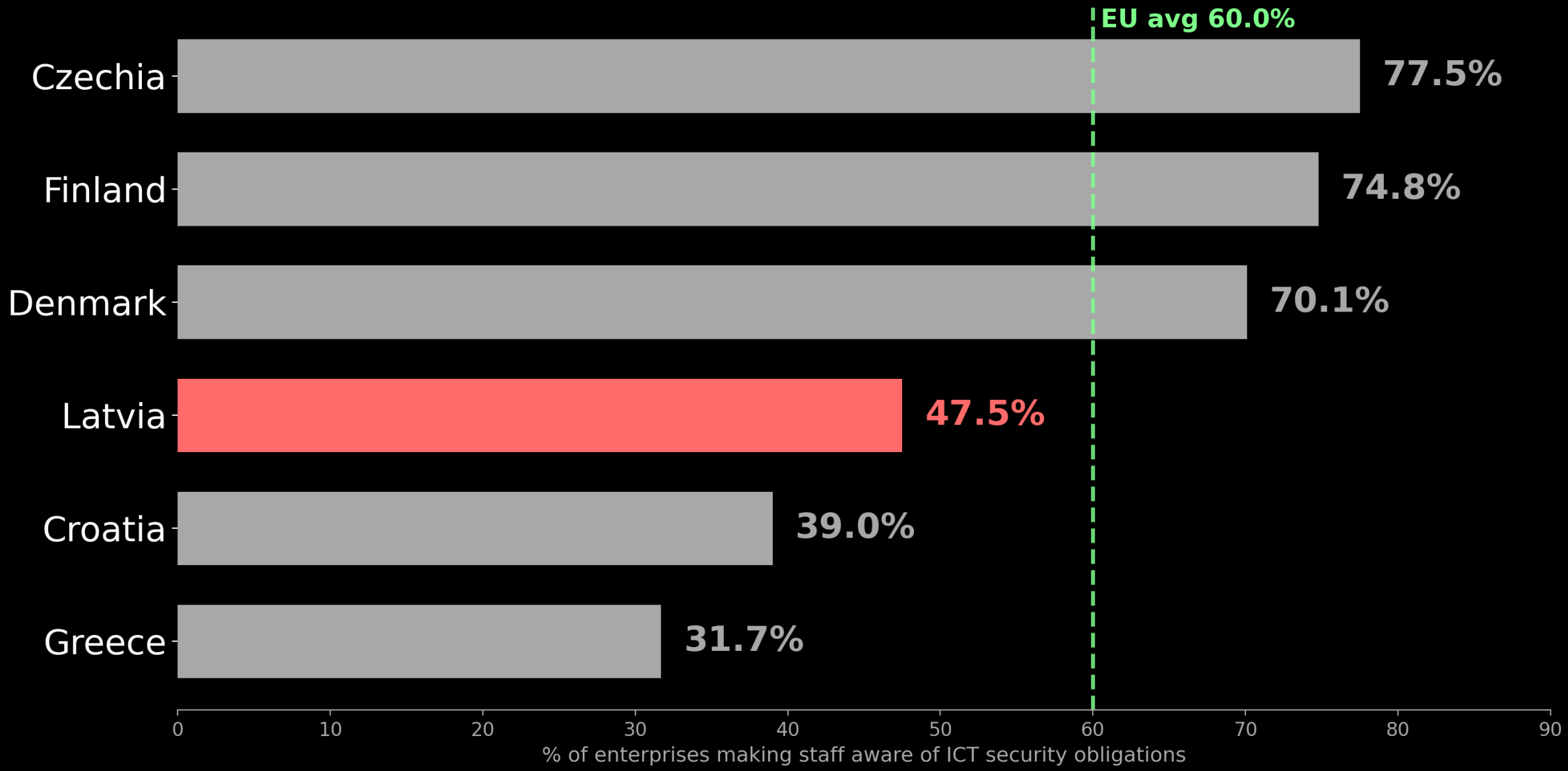
ENISA NIS Investments 2024

68%

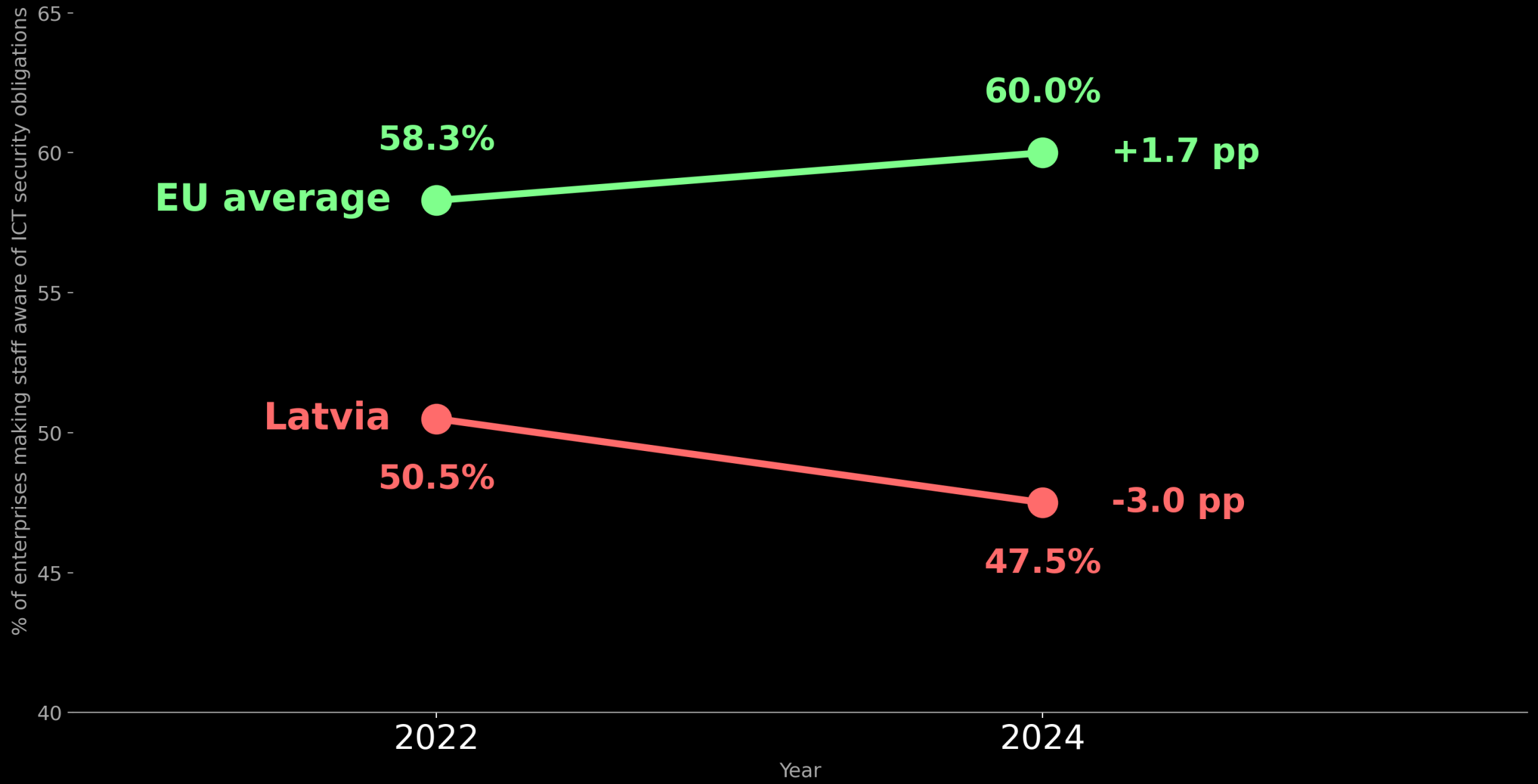
Breaches still involve human error

Plateaued for 5+ years

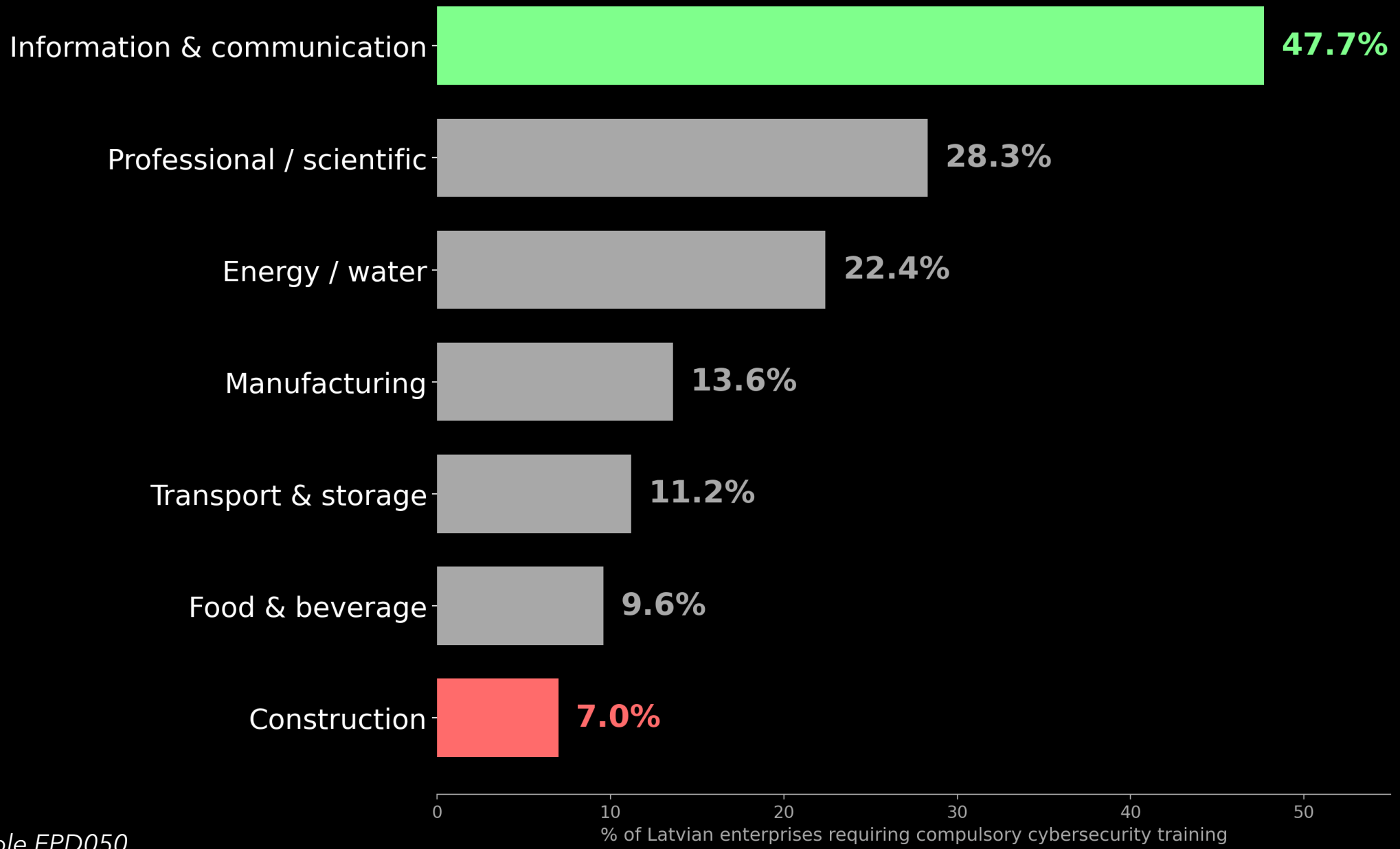
Verizon DBIR 2024



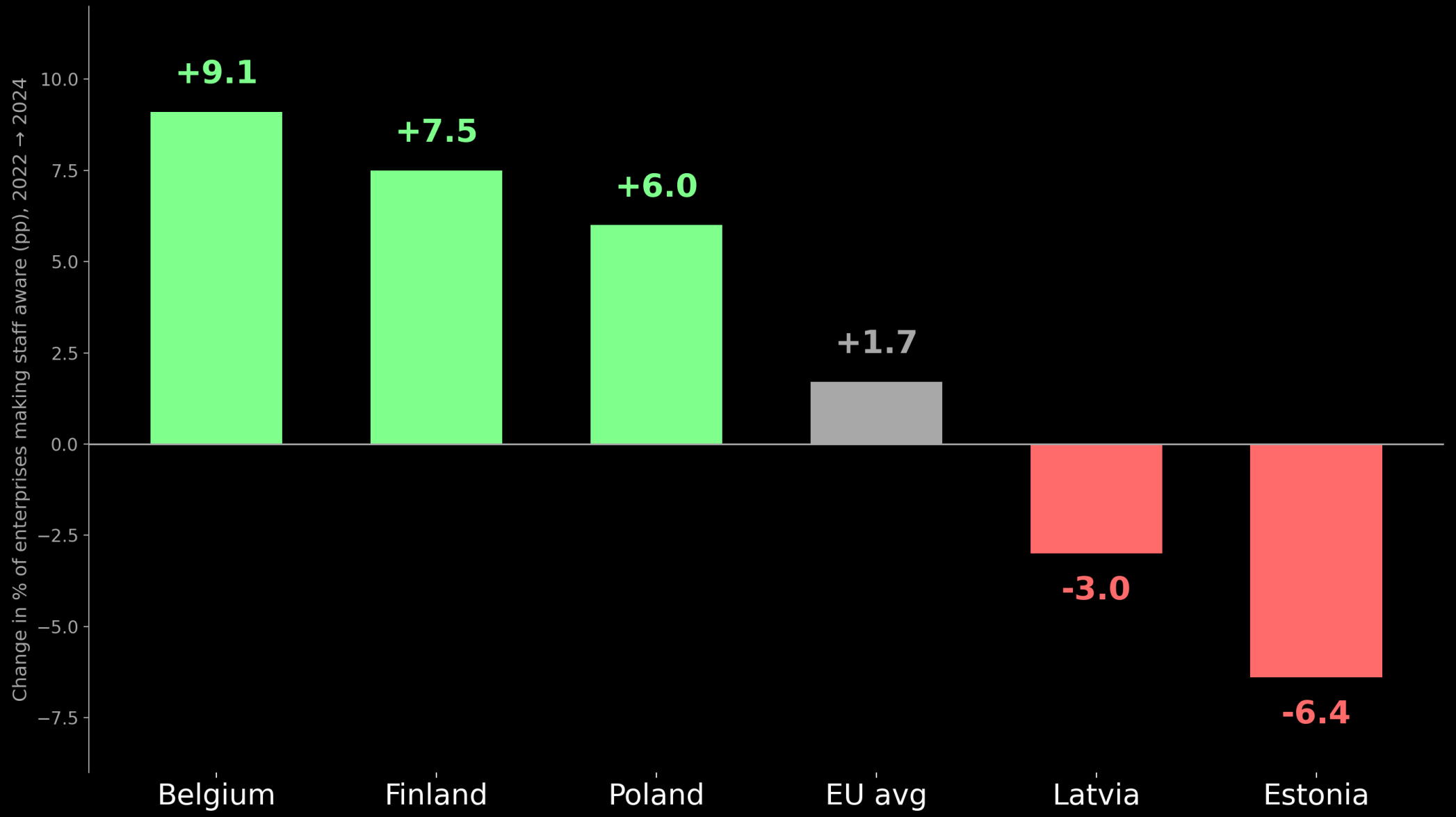
Eurostat 2024 / CSP table EPD050



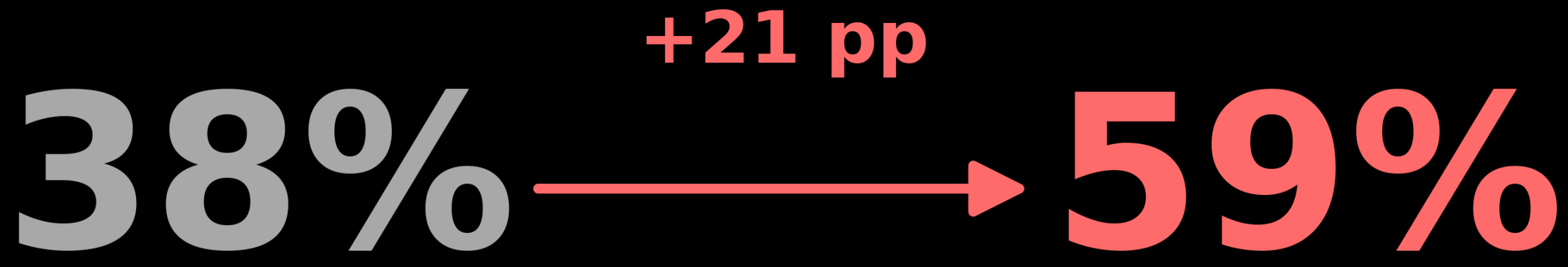
Eurostat 2024 / CSP table EPD050



CSP table EPD050



Eurostat 2024



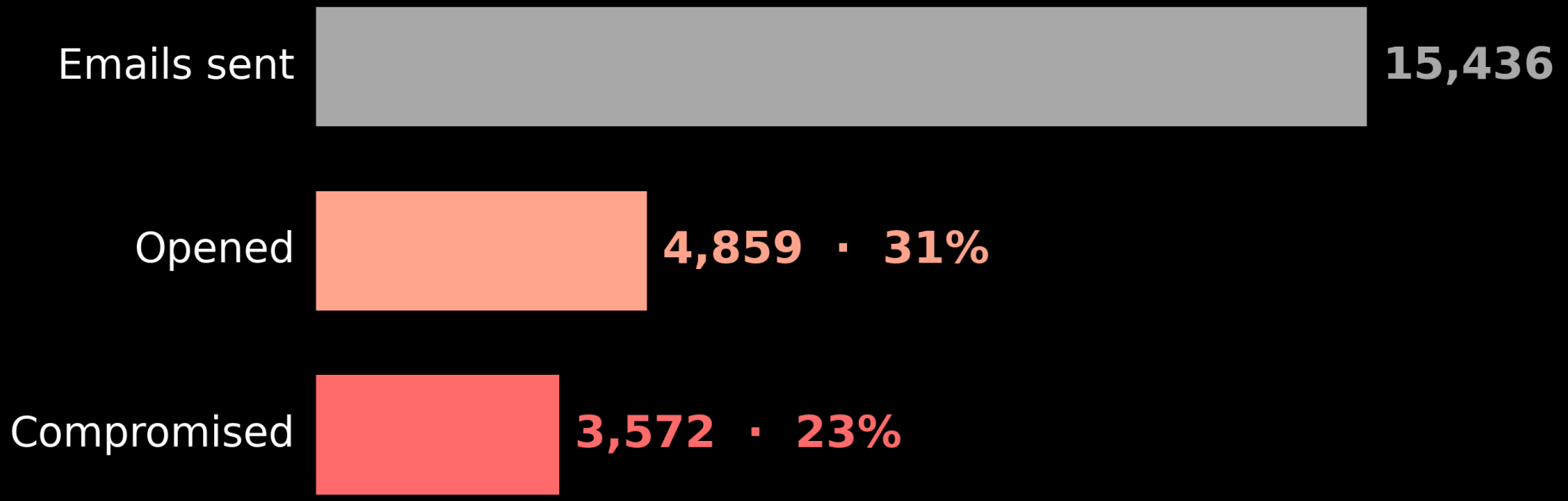
2023 2024

Share of Lithuanian cyber incidents that are social engineering

NKSC National Cybersecurity Status Report 2024

CERT.LV: THE LATVIAN RECEIPTS

14 phishing simulation campaigns in 2025



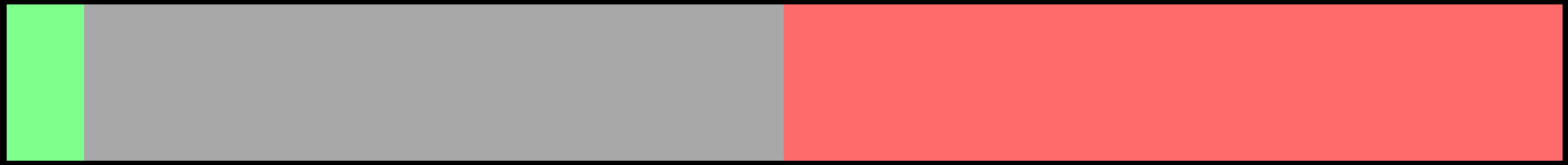
CERT.LV, 2025 (shared with permission)

AFTER BEING TOLD IT WAS FAKE...

~10%

re-entered their credentials

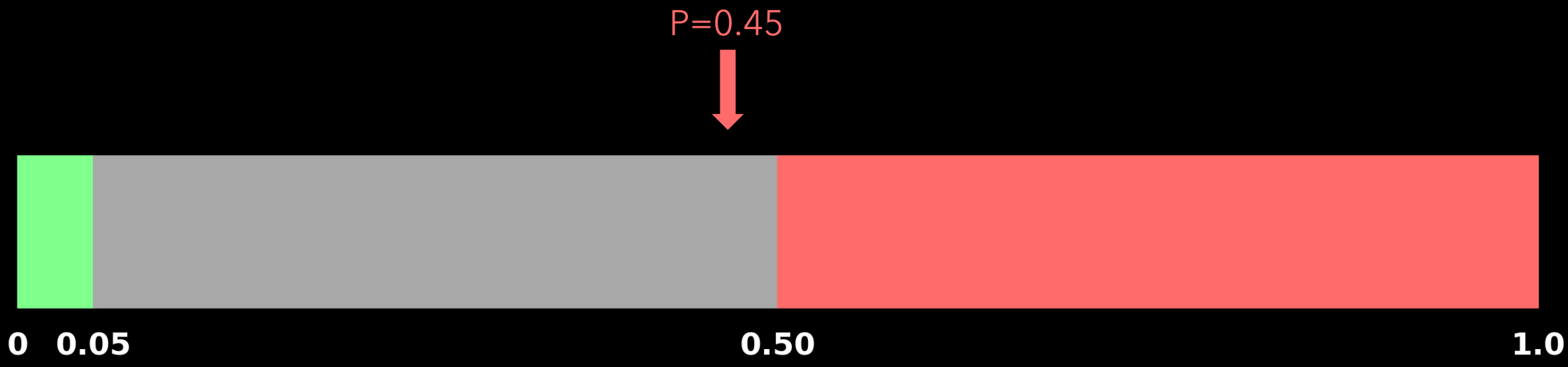
CERT.LV, 2025 (shared with permission)


0
0.05
0.50
1.0
Real effect
Maybe
Just noise

NO EFFECT

Untrained: 9.8%

Trained: 10.5%



Rozema & Davis, USENIX Security 2026

N = 12,511 employees

THE ETH STUDY

14,000 employees *15 months* *real working email*

"Embedded training during simulated phishing exercises does not make employees more resilient to phishing — it can have unexpected side effects that make employees even MORE susceptible."

Training did not fail to help.
It actively made people worse.

Lain, Kostiainen & Čapkun, IEEE S&P 2022

69 STUDIES META-ANALYSIS

Effect on knowledge

Cohen's d = 1.02

Effect on behaviour

Cohen's d = 0.36

"We have become extremely good at changing precursors to behaviour, but not the actual behaviour."

Prümmer, van Steen & van den Berg, Computers & Security 150, 2024

THEY CLICK ANYWAY

68%

of employees admit they knowingly took risky actions despite training.

Proofpoint State of the Phish 2024 · n=7,500 employees, 15 countries

WE WOULD NEVER TOLERATE THIS ELSEWHERE

Your accountant doing penetration testing.

Your CISO doing brand marketing.

A tax accountant teaching financial literacy in schools.

Why is cybersecurity the exception?

THREE MISMATCHES

Cybersecurity people are great at cybersecurity.

They are being asked to do three things they were never trained for:

1. Talk to non-techies
2. Teach
3. Stay current *AND* deliver behaviour-change

KNOWING IS NOT TEACHING!!!

"Pedagogical Content Knowledge:
knowing the topic and being able to teach the topic
are different professional competencies."

One does not imply the other.

Shulman, Educational Researcher 1986 · Harvard Educational Review 1987

CURSE OF KNOWLEDGE

Maths teachers with the MOST subject expertise

made the WORST predictions

about what novices find difficult.

The more expert you are, the harder it is to remember being a beginner.

Nathan & Petrosino, American Educational Research Journal 2003

"They understand technology and problems so well, they assume other people must understand it also... they communicate in rather confusing terms."

"Non-technical skills are deemphasized in cybersecurity training, limiting career progression."

– Haney & Lutters, Information & Computer Security 29(3), 2021
NIST researcher · n=28 grounded-theory interviews

ACCIDENTAL CYBERSECURITY

76% hold no formal cybersecurity qualification

57% took the role on top of an unrelated job

34% transitioned from non-cyber roles entirely

Flash Eurobarometer 547, 2024 · EU staff in cybersecurity-responsible roles

ENISA'S OWN FRAMEWORK

12

distinct cybersecurity professional roles

Labelled "security awareness educator" or "trainer":

1*

ENISA European Cybersecurity Skills Framework, 2022

**Originally when presenting there was number 0 but I was corrected so slide also now shows correct number*

"Existing IS-security training approaches
do not meet basic pedagogical requirements."

Nothing has changed.

Karjalainen & Siponen, Journal of the AIS 12(8), 2011

NO SPARE BANDWIDTH

11.9% → 11.1%

IT FTEs on info security · 4th annual decline

89%

expect they need MORE cyber staff for NIS2

59%

of SMEs struggle to fill cyber roles at all

ENISA NIS Investments 2024 · n=1,350 EU organisations

BURNOUT

48%

report exhaustion

47%

feel overwhelmed

Half the profession.

ISC2 Cybersecurity Workforce Study 2024 · n=14,865

WHERE THEIR TRAINING TIME GOES

Skill gaps they report:

AI/ML security · Cloud · Zero trust · AppSec · IR

Skills not on anyone's CPE budget:

Instructional design · Adult learning theory
Behavioural science · Communication for non-experts

ISC2 2024 · ENISA ECSF role profiles

INDUSTRY FOCUS

Where billions go:

CISSP
OSCP
CEH
GIAC
SANS
MIT / ETH
cyber MBAs

Who actually gets phished:

Board members
CEOs
Developers
Sysadmins
Finance / AP
HR / Reception
Everyone else

ENISA ECSF

"Terrible. Really just horrible.
I'd need a red-hot poker
and open up my eyes,
it's so boring."

An Australian employee, describing his cybersecurity training

Reeves, Calic & Delfabbro, Computers & Security 106, 2021

COMPLIANCE BUDGET

Employees have a finite "compliance budget" –
a tolerance for security demands that depletes
every time policy or training imposes friction.

Once it's spent, they stop complying.
Regardless of training.

Beautement, Sasse & Wonham, NSPW 2008

MORE TRAINING, LESS COMPLIANCE

Negative correlation

between frequency of cybersecurity training
and employee compliance.

More mandates → more burnout → more violations.

Reeves, Calic & Delfabbro, Computers & Security 128, 2023 · n=457

PUNITIVE SIMULATIONS

Phishing simulations with enforced training and punishment for failure:

- **Harm employee psychological wellbeing**
- **REDUCE reporting of real phishing**
- **Damage productivity**

CREST research

TRAINING IS NOT ZERO VALUE

IBM 2024: orgs WITH training averaged $4.15M / breach

vs $5.10M WITHOUT. (correlational, not causal)

KnowBe4: simulation click-rate falls 34% → 4.6% over 12 months

(vendor data · measures simulations, not real-world resilience)

We are measuring the wrong things.

TOOLING BEATS TRAINING

Same 14,000-employee ETH study that found training backfiring.

Email warning banners.

A "report phishing" button.

Both were highly effective.

Lain, Kostiainen & Čapkun, IEEE S&P 2022

ENISA

"Cyber threat awareness campaigns alone do not provide sufficient protection.

Organisations must exceed the minimal compliance approach."

The mismatch is structural.

The fix is not on this slide.

Daniels Heincis · BSides Riga 2026