InCyS4.0

Industrial Cyber Security 4.0

Erasmus+ Project

Authors

João Rebhan · **Prof. Nuno Escudeiro**

Instituto Politécnico do Porto (IPP), Portugal

Partner Institutions

IPP — Instituto Politécnico do Porto, Portugal · Politeknika Txorierri, Spain · Hellenic Mediterranean University (HMU), Greece

Erasmus+ Programme | 2024–2026

Cybersecurity in Industrial Environments

Awareness & Readiness Assessment

Survey-based study · n=815 participants
(n=224 operational technicians · n=591 general workers)

815	224	591	3
Participants	Technicians	Workers	Countries

Agenda

01 Context & Research Questions

02 Portugal on the Cybersecurity Map

03 Methodology

04 Technicians — OT/ICS Security Practices

05 Workers — Human Risk Behaviours

06 Security Maturity by Company Size

07 Key Findings & Recommendations

Context & Research Questions

Why does this matter?

- Industry 4.0 merges IT and OT — factory floors are now cyber targets
- ENISA: 68% of European OT environments lack network segmentation
- Human error accounts for 74% of breaches (Verizon DBIR 2023)
- No large-scale empirical study on OT cyber readiness in Portuguese SMEs

RQ 1

What OT/ICS security measures are deployed by industrial technicians?

RQ 2

What cyber-risk behaviours do general workers exhibit?

RQ 3

How does company size correlate with cybersecurity maturity?

Portugal on the Cybersecurity Map

300+

incidents reported to CNCS in 2023

900%

increase in OT ransomware 2020–2023

NHS

Hospital de Braga (2023) — weeks offline after cyberattack

TAP

Data breach (2022) — 1.5 M passengers exposed

74%

of Portuguese SMEs have no incident response plan

NIS2

EU directive transposed into Portuguese law in 2024

Methodology

Study Design

- Cross-sectional online survey (2022–2023)
- Multi-industry — manufacturing, energy, utilities
- Two separate questionnaires:
- Technicians — 14 items (OT/ICS practices)
- Workers — 12 items (IT behaviour)
- Statistics: proportions with 95% confidence intervals + chi-square tests

n = 224

Operational Technicians

OT/ICS questionnaire

n = 591

General Workers

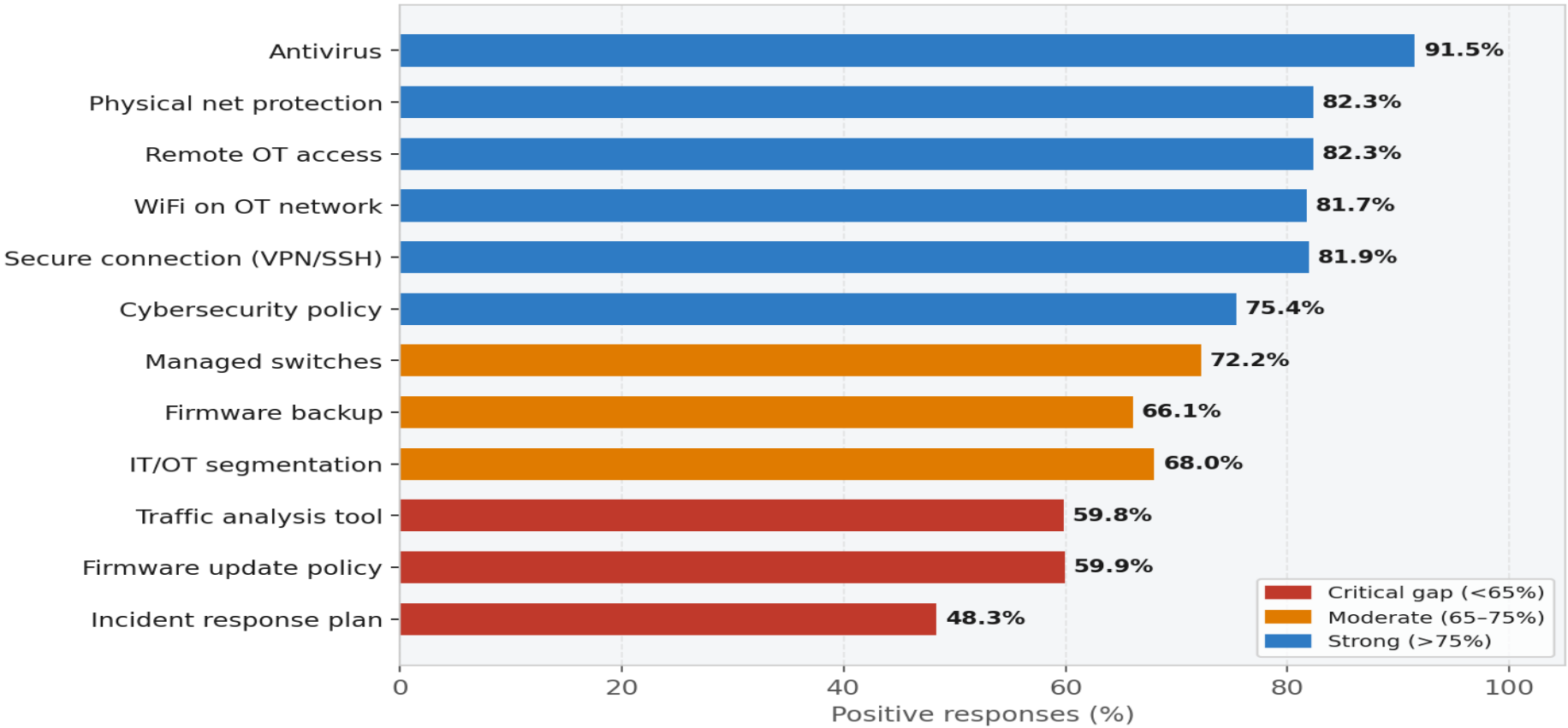
IT behaviour questionnaire

n = 150

Companies with formal security policy

Sub-group analysis

OT/ICS Security Practices — Technicians (n=224)



Critical OT/ICS Gaps

48.3%

Incident Response Plan

Fewer than half have a tested IR plan

59.9%

Firmware Update Policy

Patch hygiene remains inconsistent

59.8%

Traffic Analysis Tool

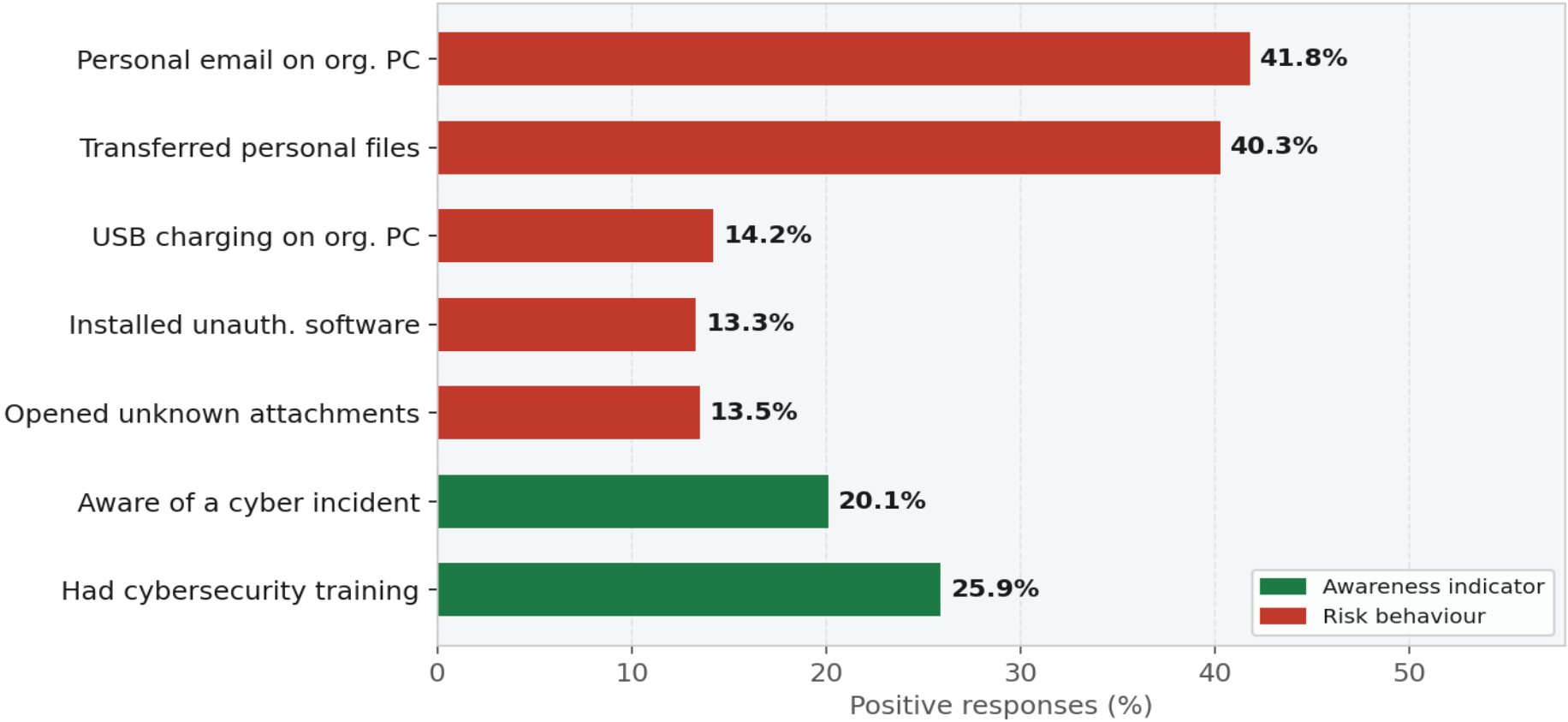
No anomaly detection in ~40% of sites

68.0%

IT/OT Segmentation

Flat networks still common in SMEs

Human Risk Behaviours — Workers (n=591)



The Human Element

1 in 4

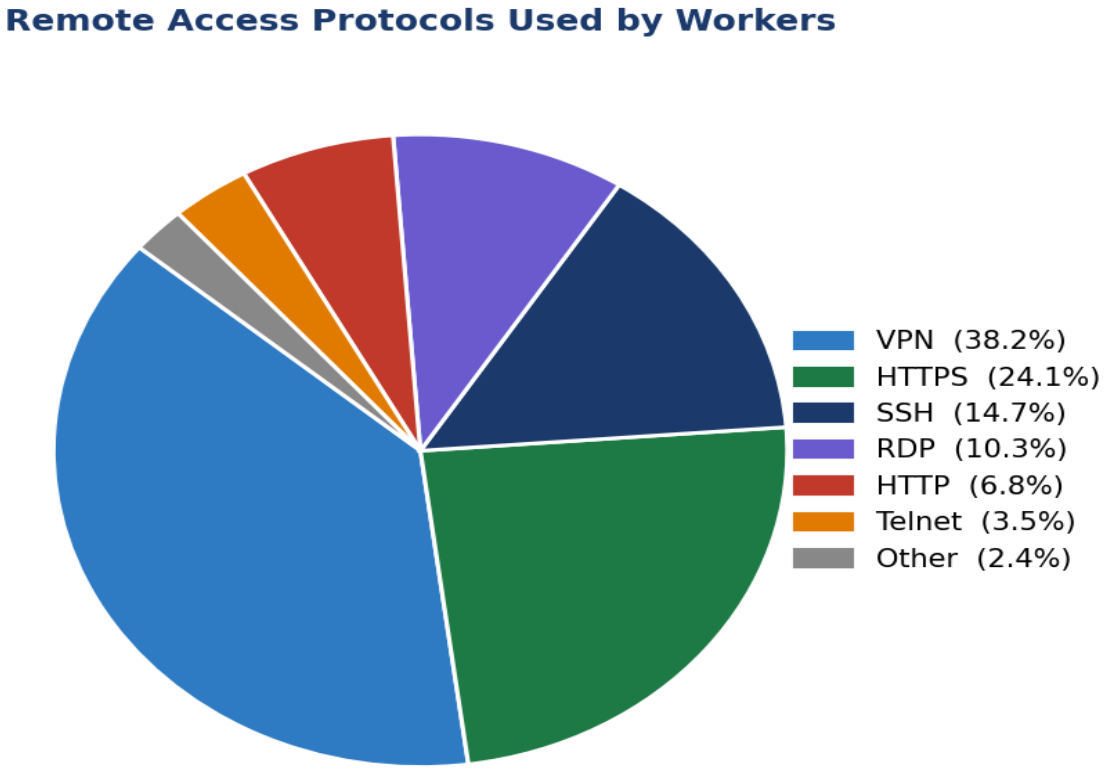
workers received
any cybersecurity training

Only 20.1% are aware of a cyber incident
in their own organisation

Top Risk Behaviours

41.8%	Personal email on org. PC
40.3%	Personal file transfers to org. PC
14.2%	USB charging on org. PC
13.5%	Unknown email attachment opened
13.3%	Unauthorised software installed

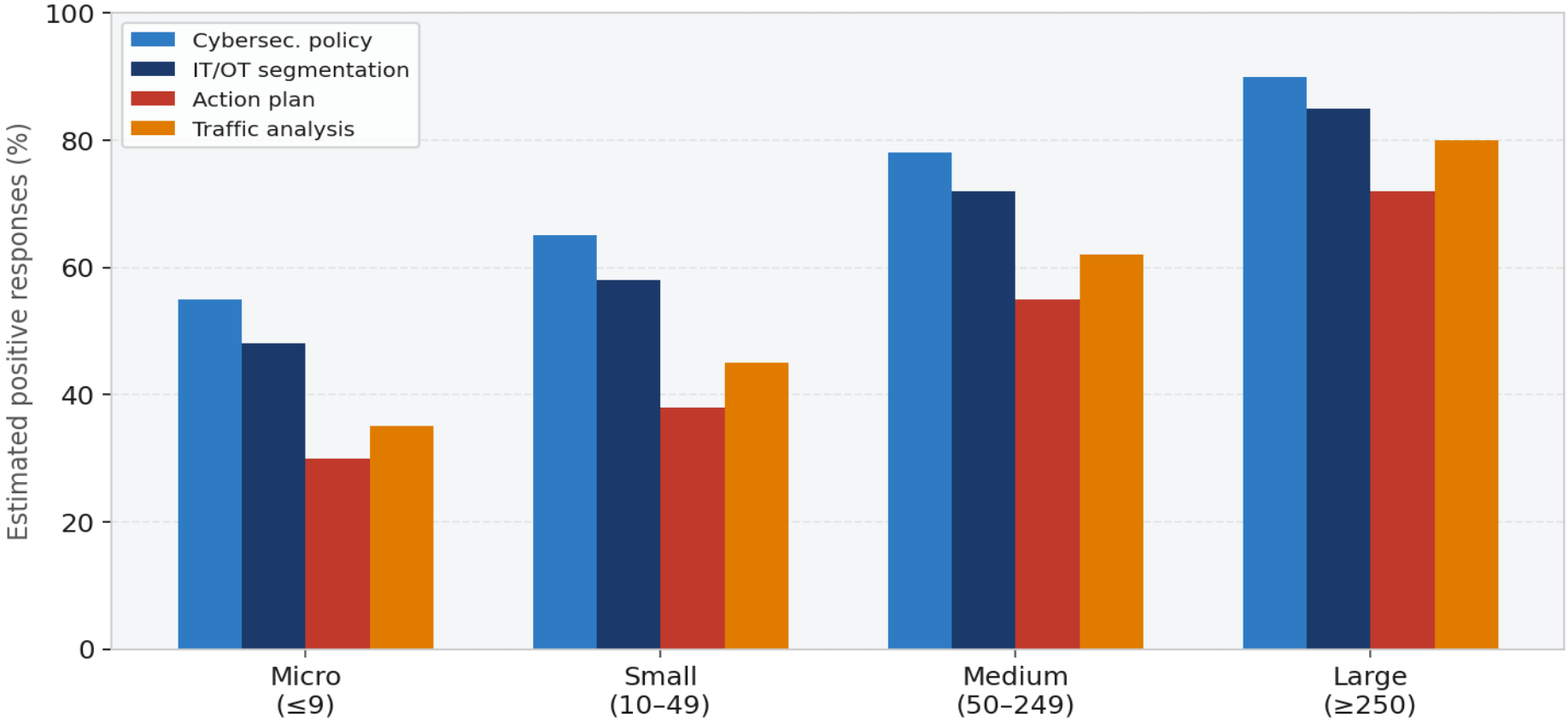
Remote Access Protocols Used by Workers



⚠ **HTTP & Telnet still in use in 2023**

VPN is dominant but not universal

Security Maturity by Company Size



Key Findings & Recommendations

OT/ICS Readiness

Antivirus adoption is high (91.5%) but foundational controls — IR plans, firmware patching, traffic analysis — are critically low. Immediate action needed.

Human Factor

Only 25.9% of workers trained. Risky behaviours (personal email, USB, file transfers) are widespread. Awareness training offers the highest ROI.

SME Gap

Micro and small firms score 20–30 pp below large enterprises on every security metric. Tailored, low-cost playbooks are essential for this segment.

Remote Access

HTTP and Telnet still present in 2023. Organisations must enforce VPN/SSH policies and audit all legacy protocols immediately.

Conclusions

InCyS4.0 Erasmus+

Portuguese industrial organisations show significant cybersecurity gaps, particularly in OT incident response planning and worker training.

Company size is the strongest predictor of security maturity — SMEs need dedicated, resource-appropriate frameworks (IEC 62443 · NIST SP 800-82).

The InCyS4.0 training curriculum was designed to address exactly these deficits across Portugal, Spain, and Greece.

Thank you