DESIGNING THE FUTURE ™

You think your Cybersecurity is complete? Here’s a few reasons why you're probably wrong.

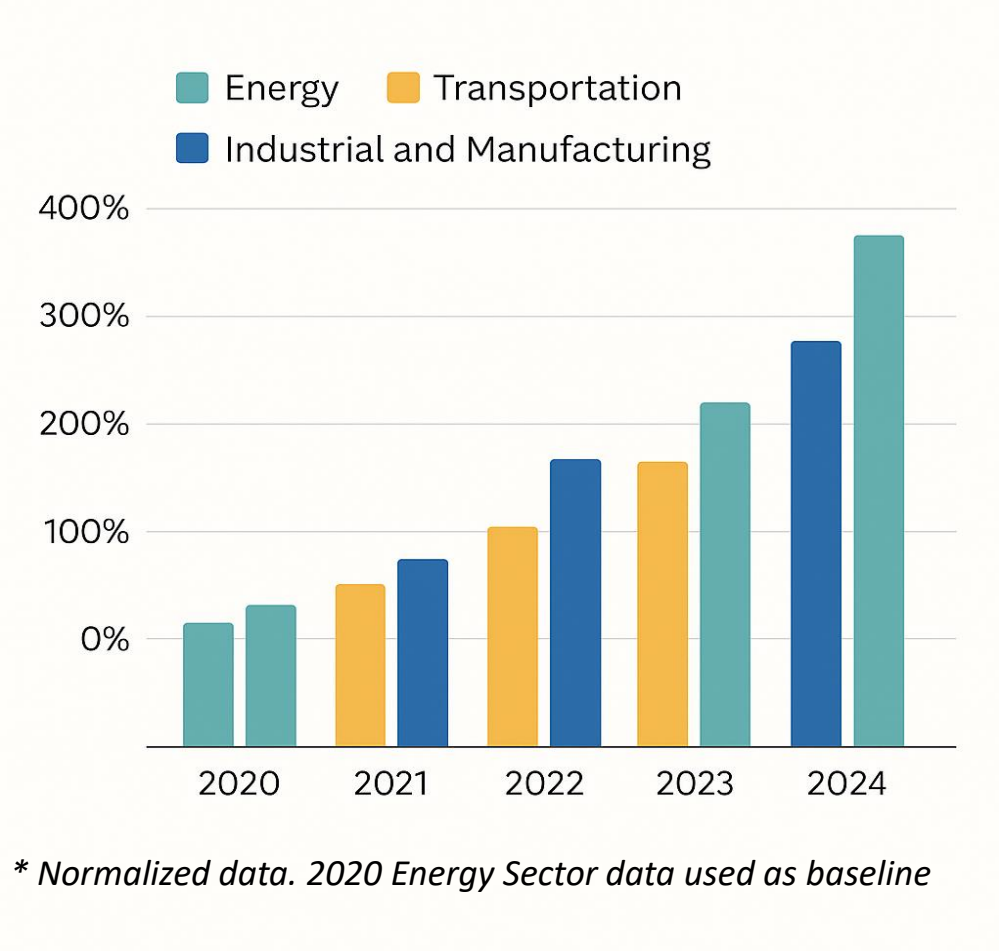
Ontario Public Transit Association

September 24th, 2025

cysca technologies

“We don’t have anything a hacker would want.”
Are you sure about that ?

Cyberattacks on Critical Infrastructures



** Normalized data. 2020 Energy Sector data used as baseline*

Energy Sector

- 2020: Baseline
- 2021: +100% (double from 2020)
- 2022: +100% (double again from 2021)
- 2023: +30% from 2022
- 2024: +70% from 2023

Transportation Sector

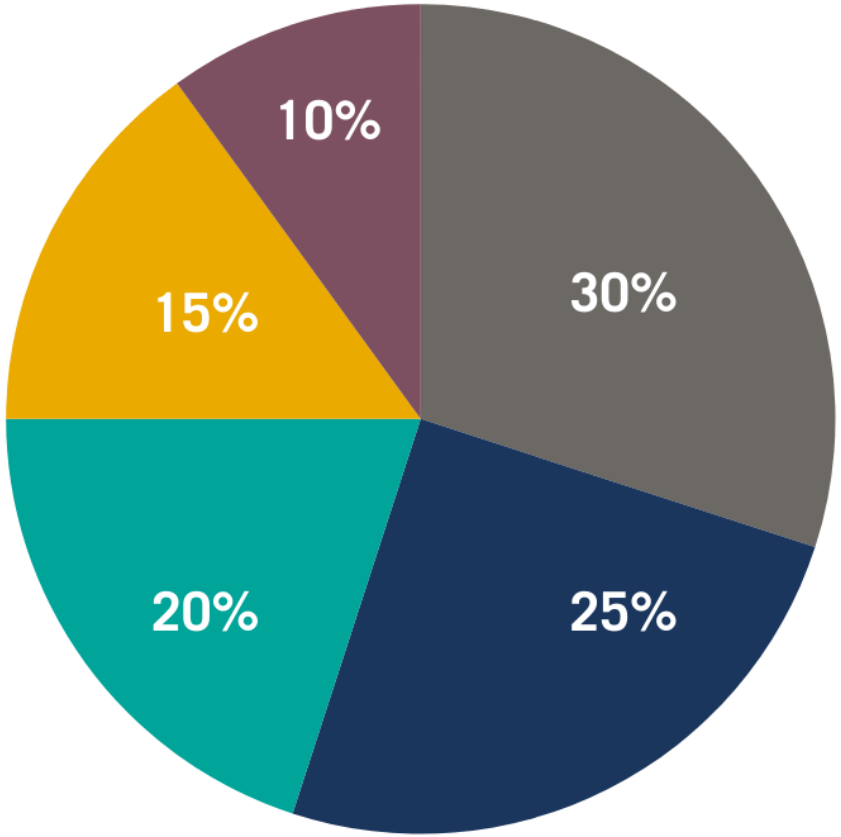
- 2022: 14 of 16 critical sectors impacted (transportation included; no specific count)
- 2023: TSA introduces new cyber regulations (contextual indicator, not numerical)

Industrial/Manufacturing Sector

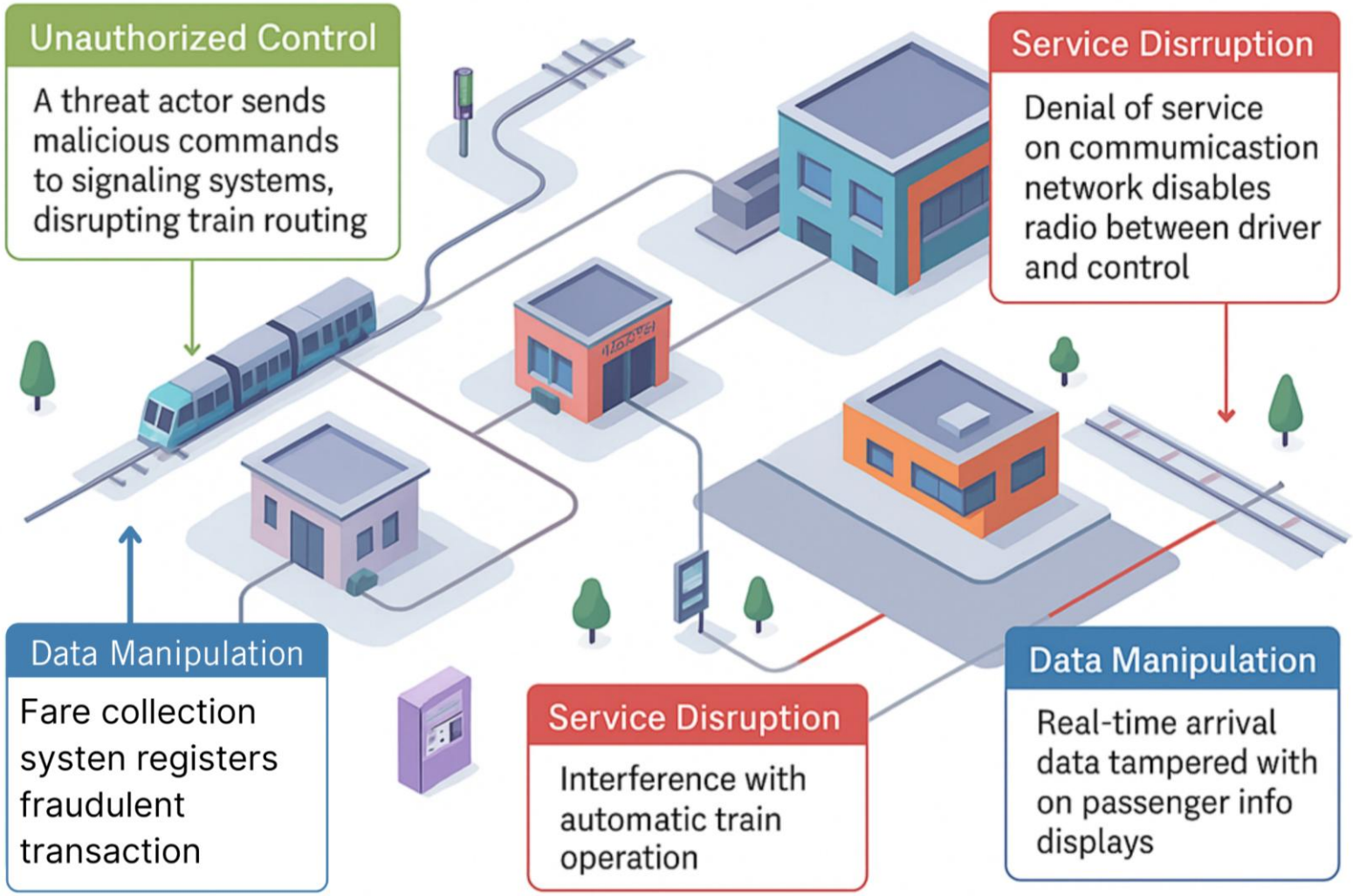
- 2022: Nearly doubled ransomware attacks
- 2024: 30% of all reported incidents from manufacturing

Cyberattacks Types

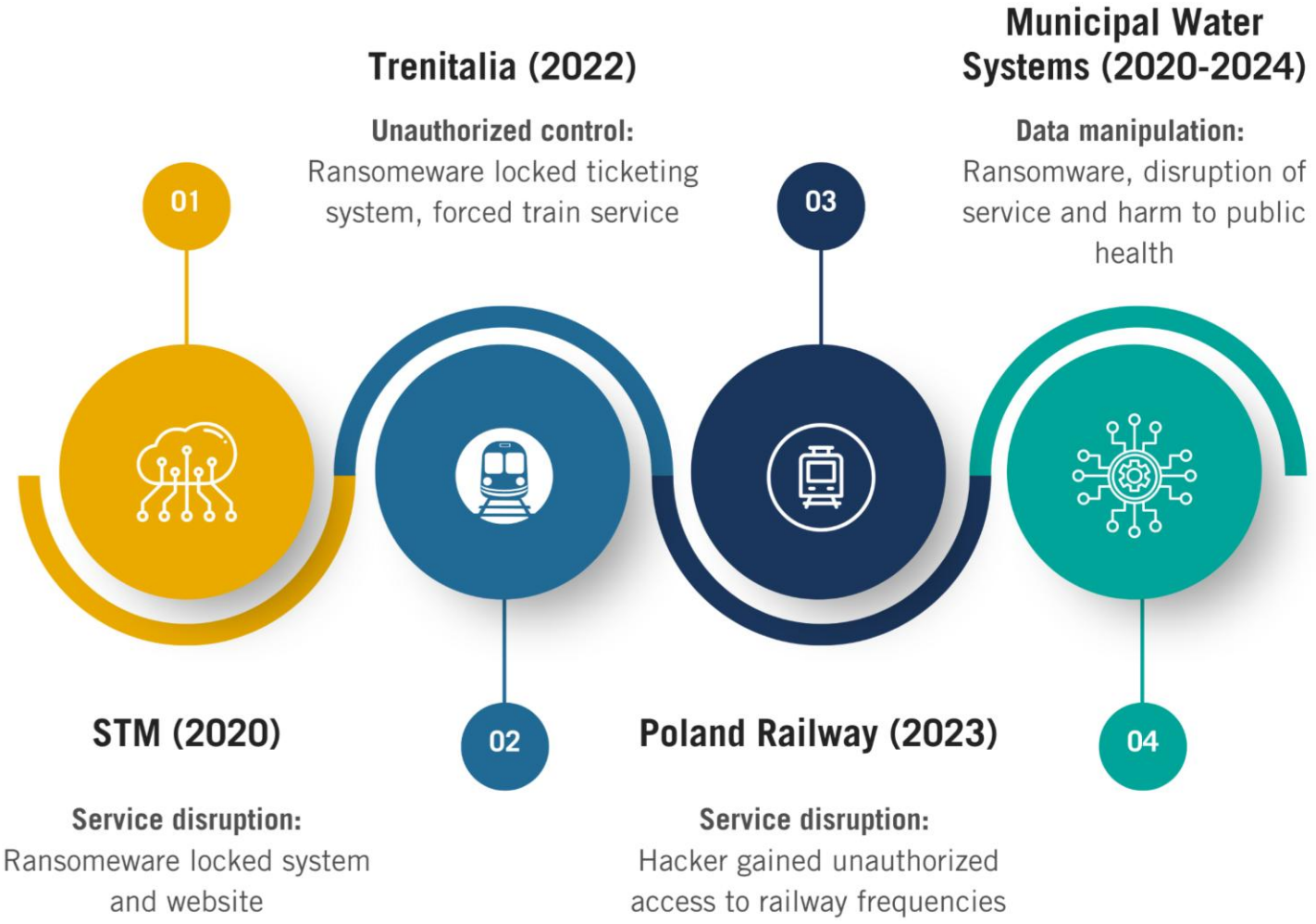
- RANSOMWARE ATTACKS
- UNAUTHORIZED ACCESS AND CONTROL
- DATA BREACHES AND INFORMATION THEFT
- DENIAL OF SERVICE (DOS) AND DISRUPTION ATTACKS
- OTHER ATTACK VECTORS



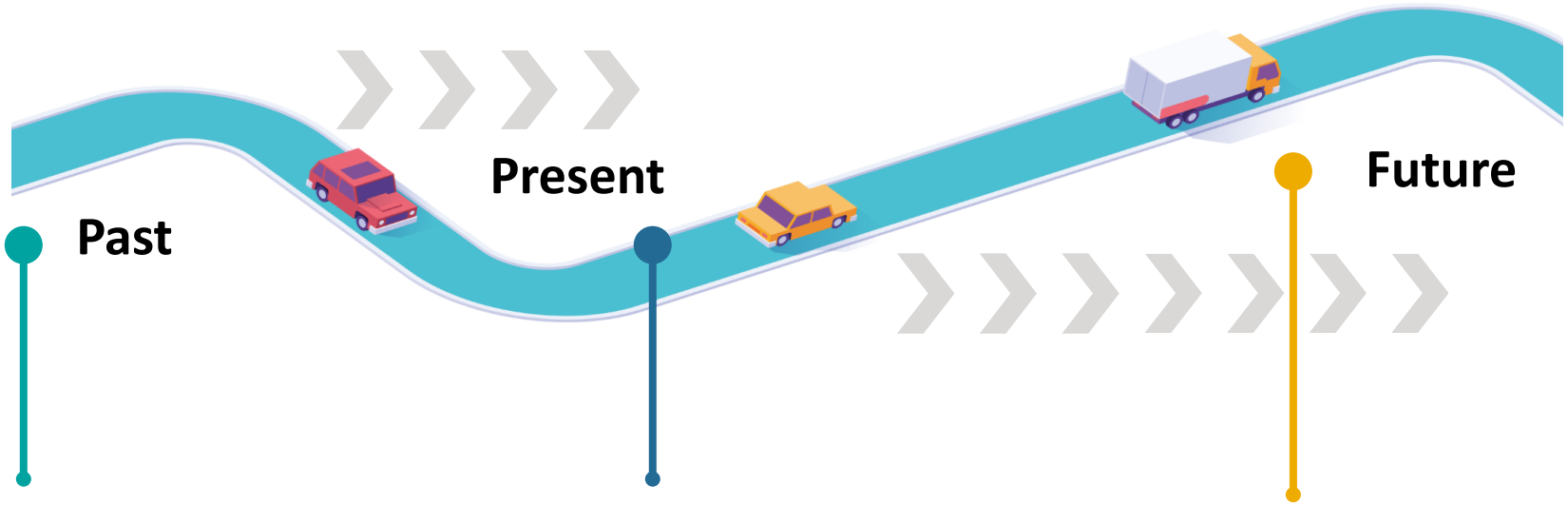
Public Transit Cyberattacks Scenarios



Public Transit Recent Cyberattacks



Evolution of Information and Operational Technologies



Completely separated networks

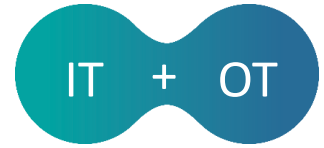
Partial network integration

Complete convergence

Information Technologies (IT)

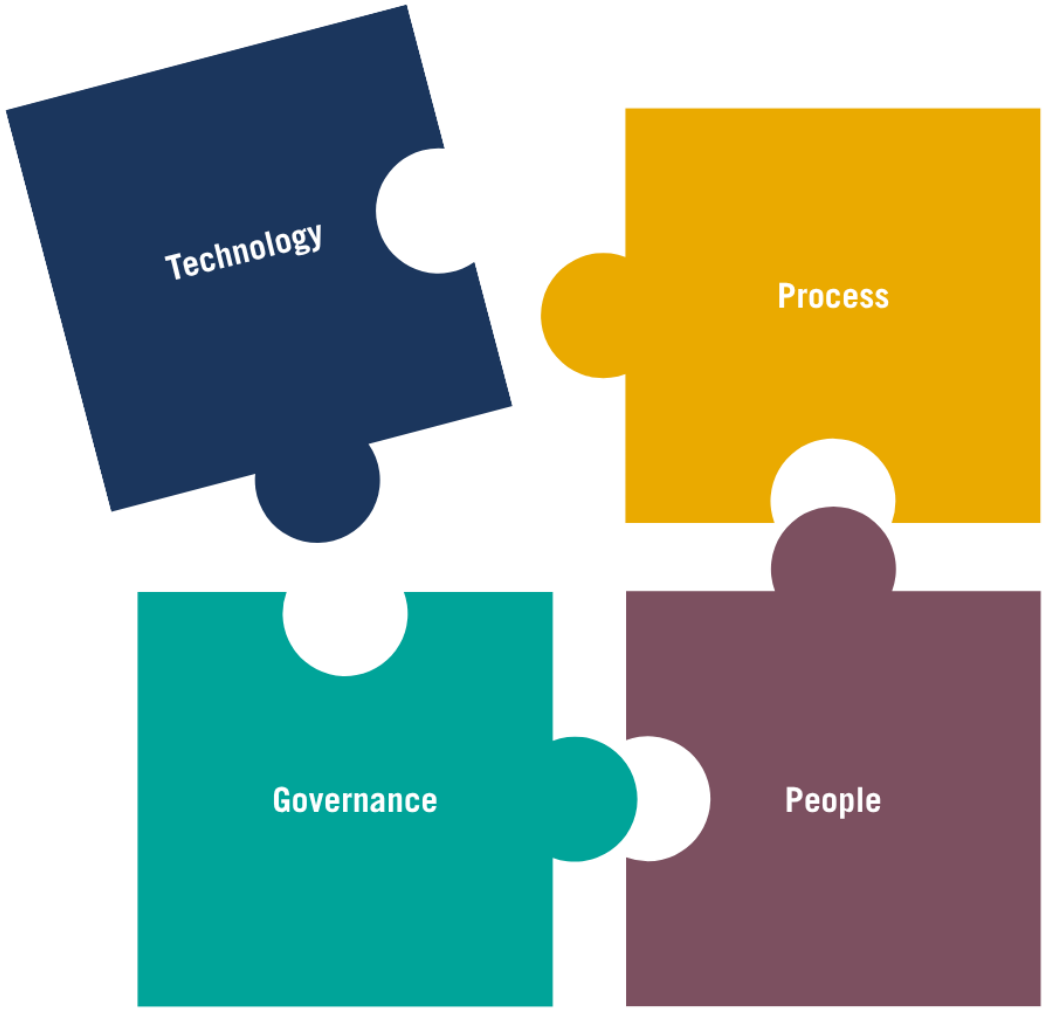
Operational Technologies (OT)

Integrated Technologies IT + OT



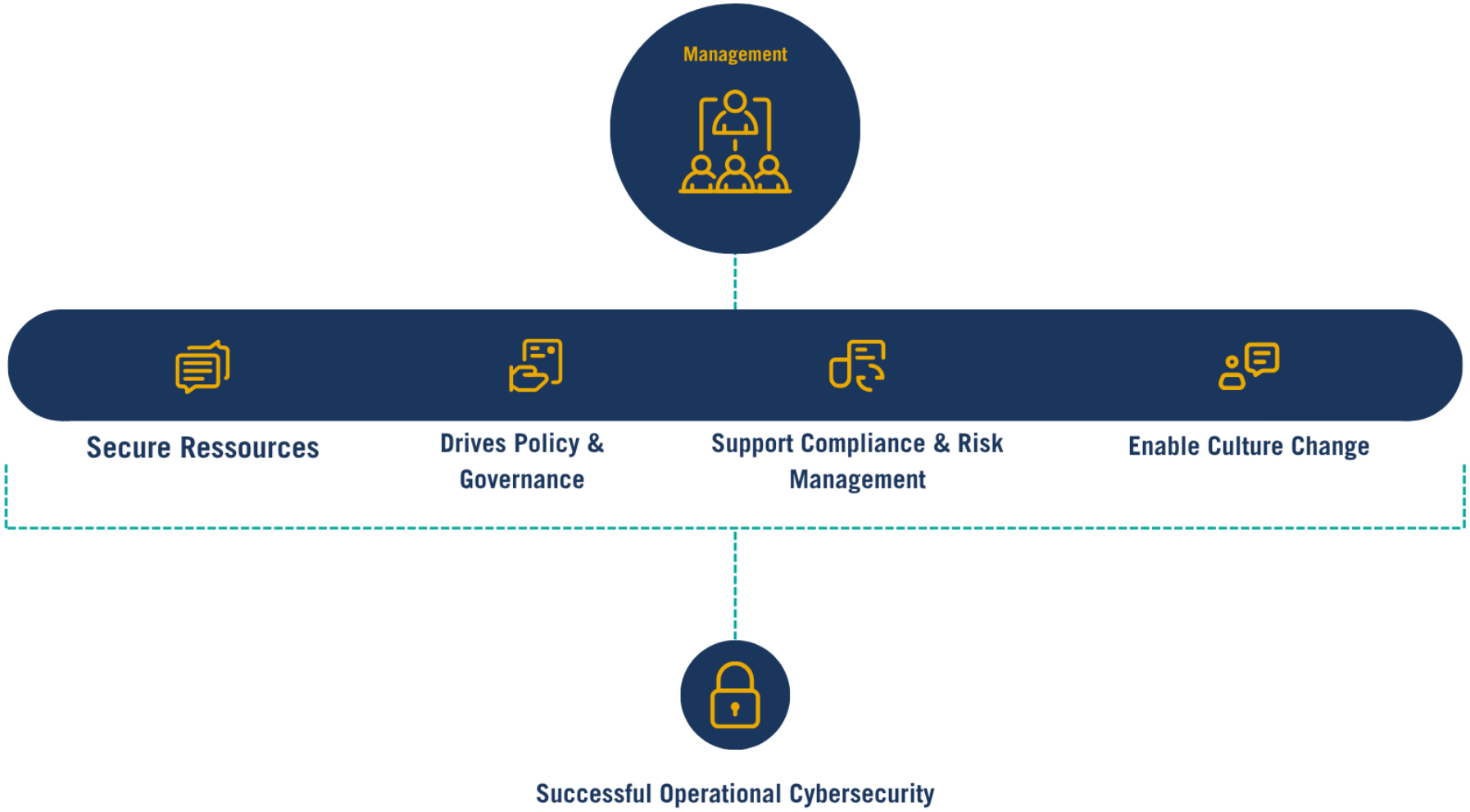
“We have a sophisticated security suite, so we’re good.”
But are you ?

Cybersecurity Pillars

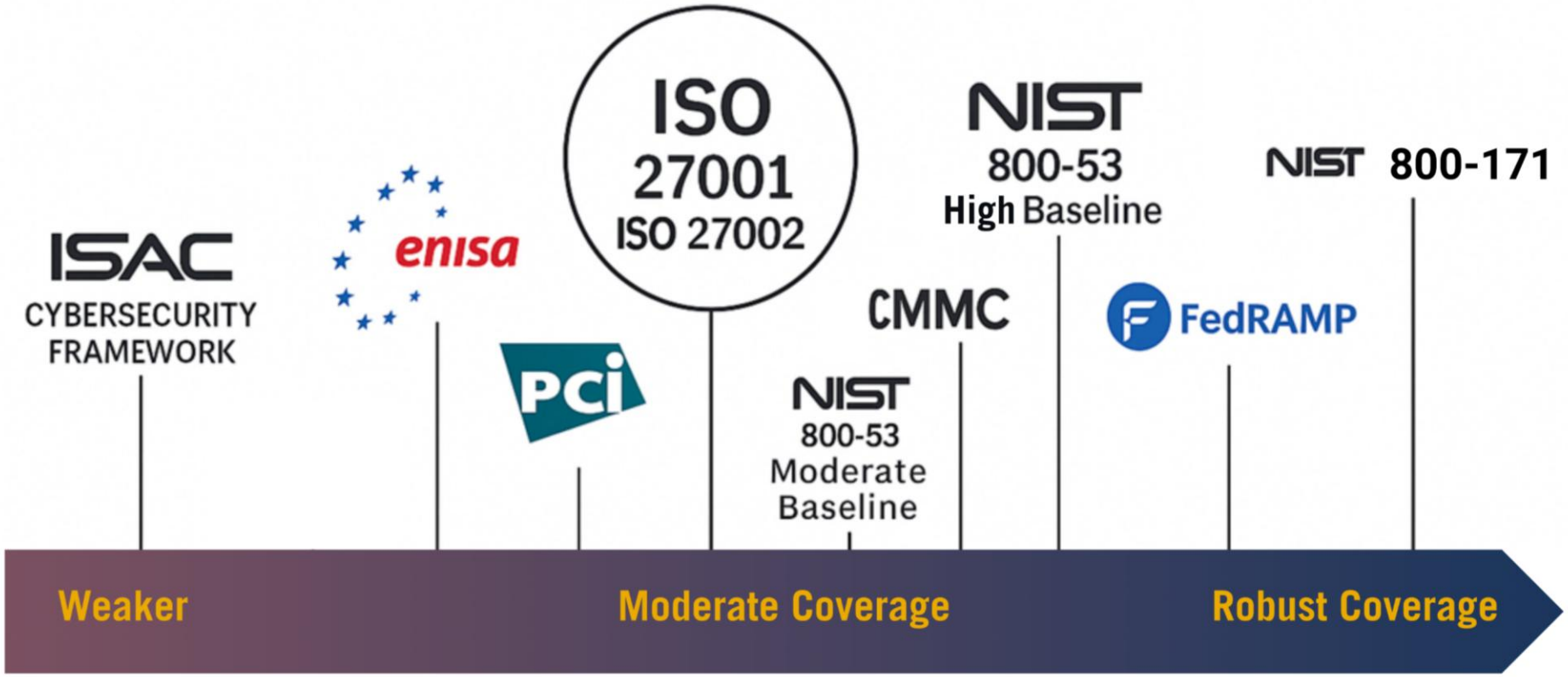


“Our IT Team takes care of that.”
They shouldn’t be the only one.

Management Endorsement is Essential



Common Cybersecurity Standards



ISO-21434 : Road Vehicules

CONCEPT:
Item definition

DECOMMISSIONING:
Lifecycle-based approach

MAINTENANCE:
Cybersecurity Maintenance Plan

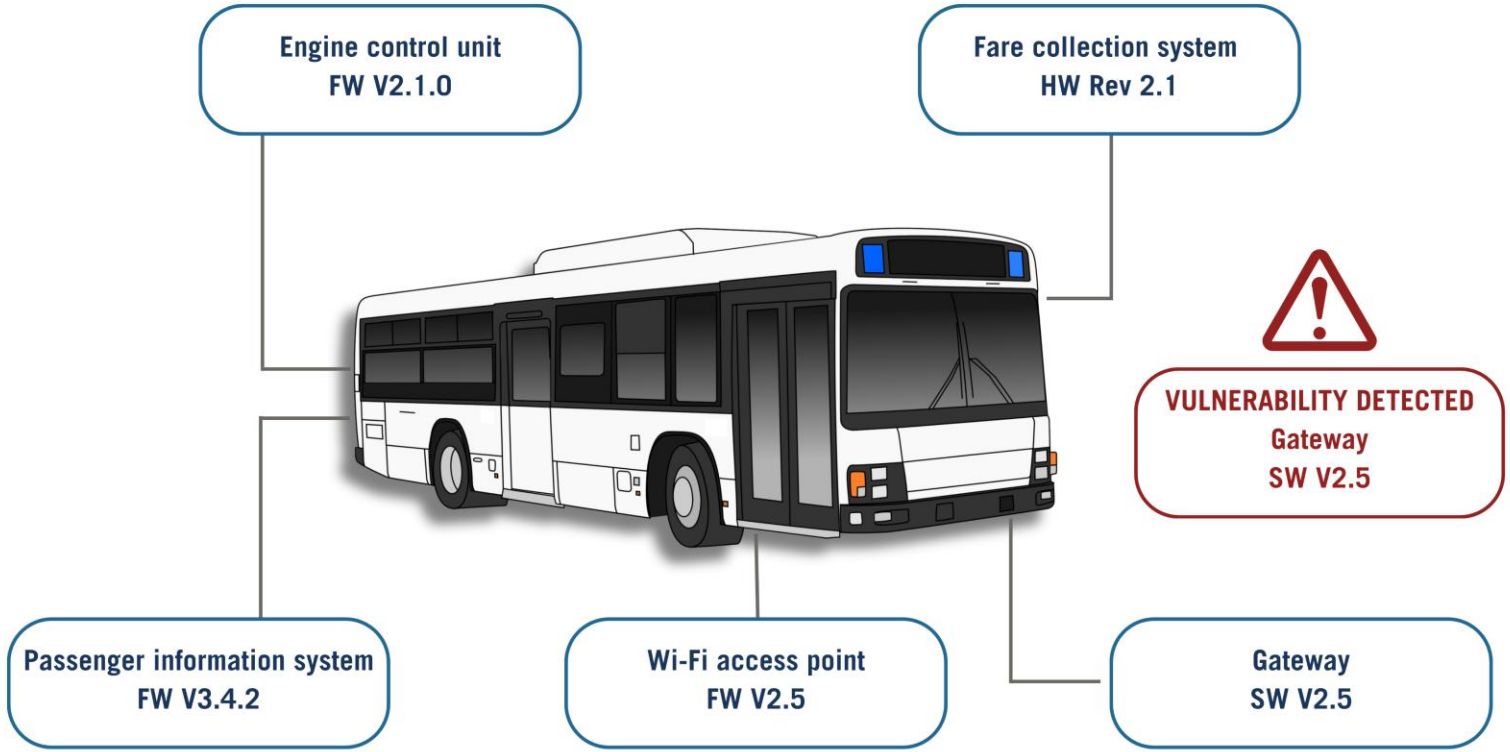
TARA:
Cybersecurity Validation Report

OPERATION:
Cybersecurity Incident Report Plan

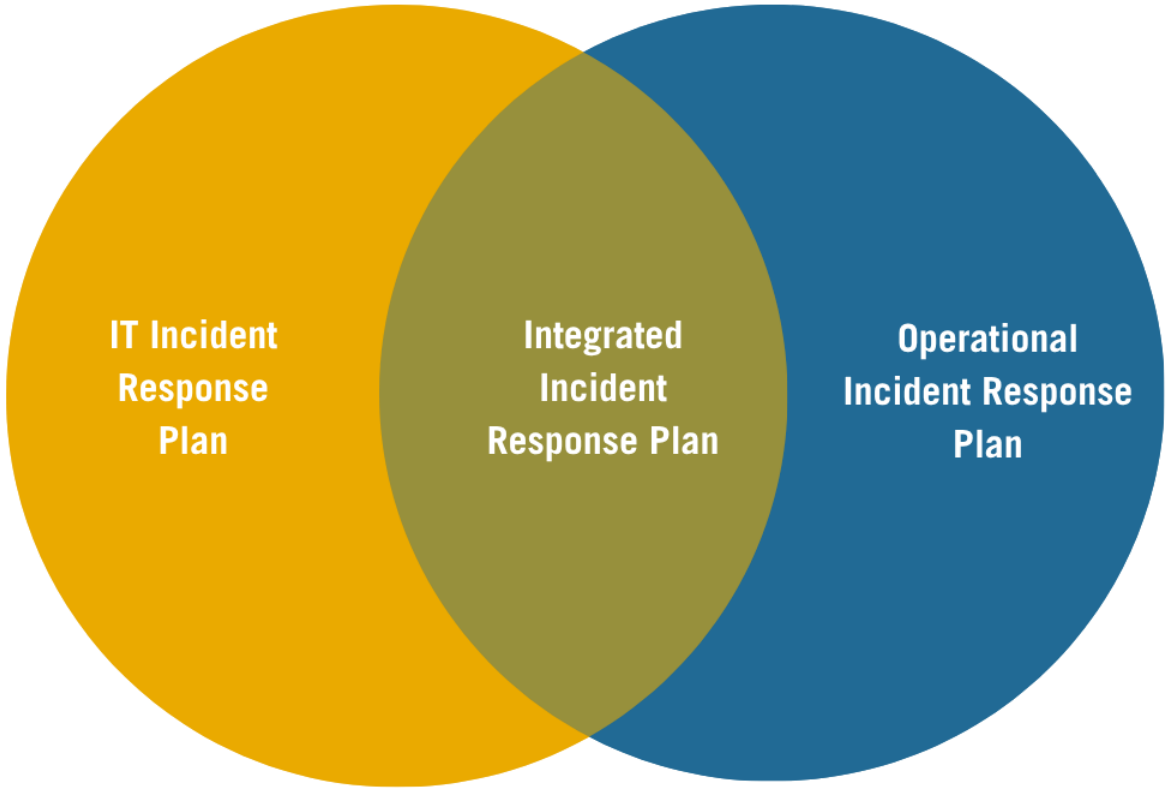
“We have performed penetration testing on our system, so we don’t need extra policies.”

Threat and Risk Assessments

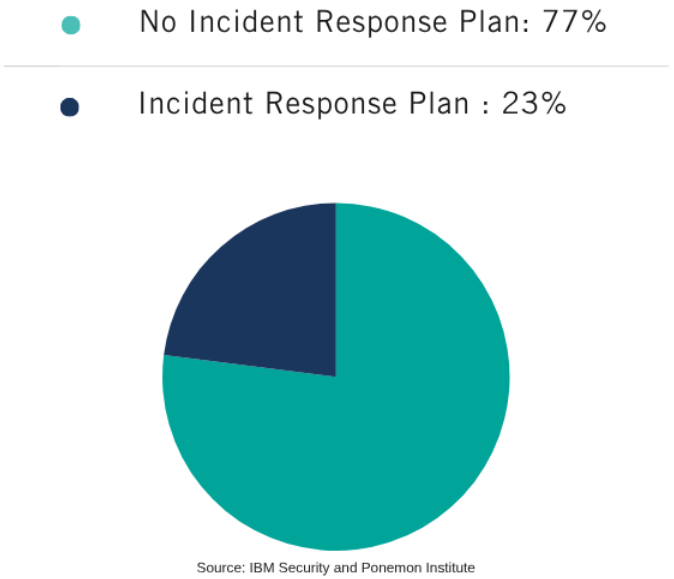
Vulnerability Management



Incident Response Plans



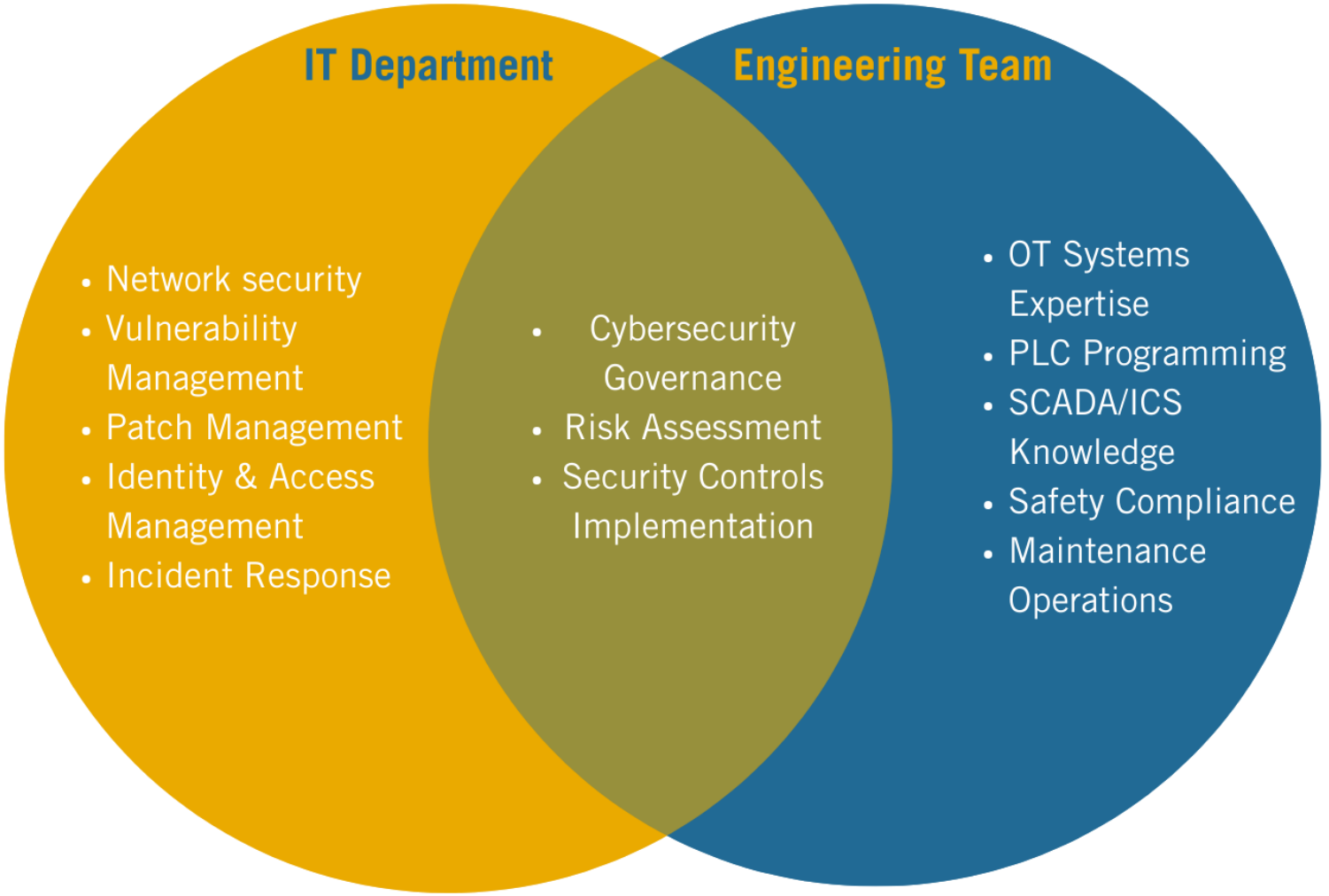
- Asset-specific response
- Engineering team roles
- Customer notification obligations
- Contractual compliace



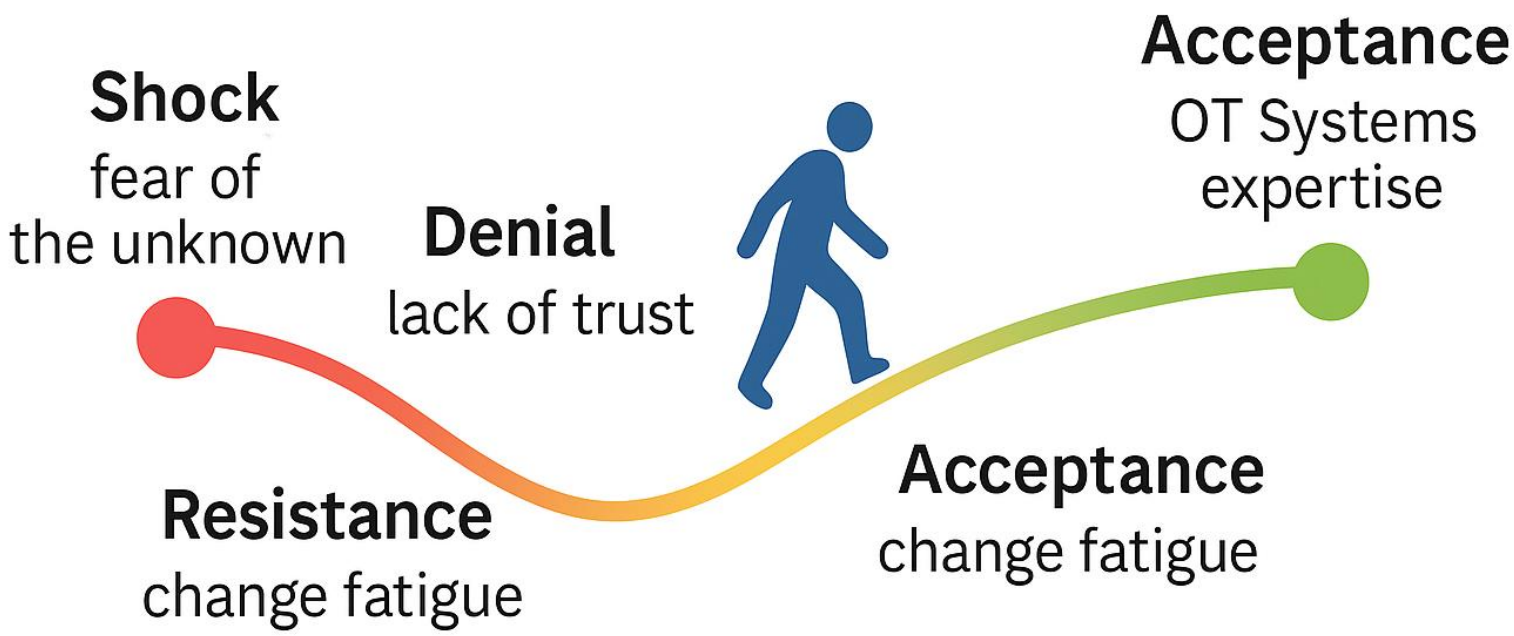
Source: IBM Security and Ponemon Institute

“Security always gets in the way of productivity.”
What if it doesn’t?

Collaboration is Key



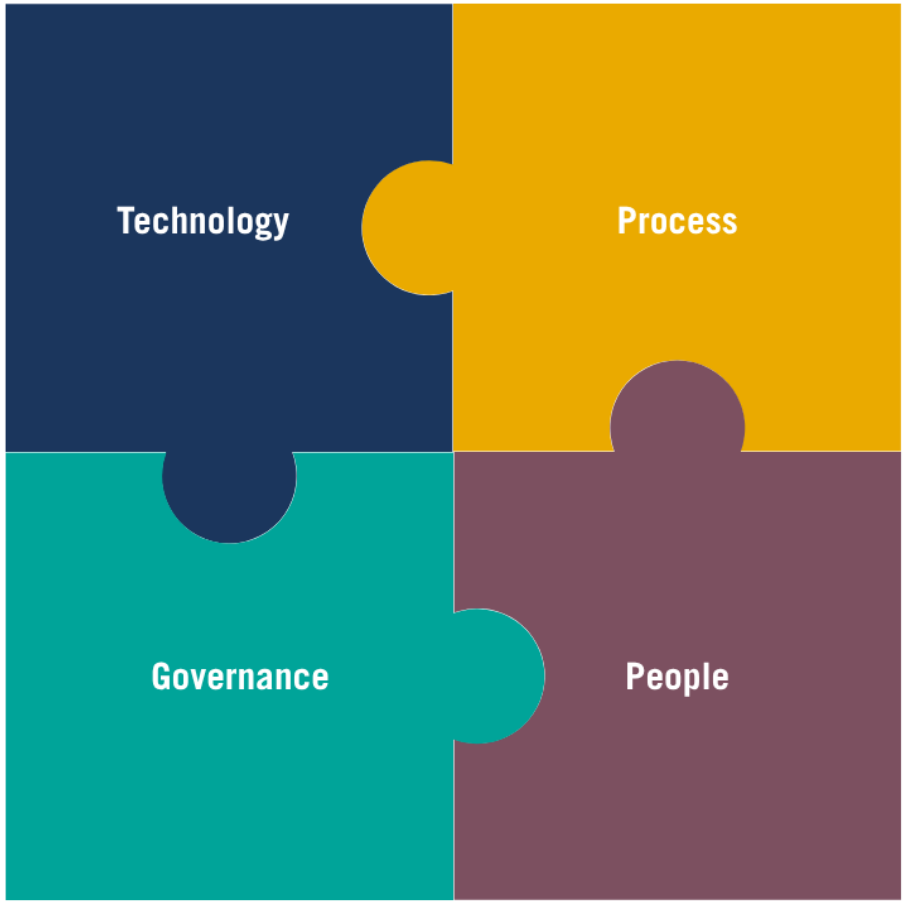
Culture Change



Training and Awareness

“Our system is not connected to the Internet.”

Not All Technology



“I didn’t know we had so many gaps until now.”
That’s where we can help.

Key Take aways

- **Cybersecurity is non-negociable**

Establish robust defenses to protect against evolving cyber threats.

- **Technology is not enough**

Adopt a holistic, organization-wide approach to resilience.

- **Leadership commitment is critical**

Ensure active engagement from executives and management.

- **Operational cybersecurity is unique**

Address real-time risks and business continuity separately from traditional IT security.

- **Policies & procecesses are foundational**

Implement clear, enforceable frameworks to support security initiatives.

- **Change management is essential**

Recognize that employee adaptation requires time, empathy, and support.

- **Success requires shared responsability**

Foster collaboration and accountability across all levels of the organization.

Thank you, any questions ?

Contact us: sales@cysca.com