Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Contrasted gaps: Common Solutions in a Global OT Environment

Industrial Cybersecurity Center

Susana Asensio

Agenda

Contrasted gaps: Common Solutions in a Global OT Environment

Who is CCI & Why CCI has the capacity to detect global gaps

More remarkable contrasted gaps and their consequences

Initiatives to decrease these barriers

CCI
The Industrial Cybersecurity Center

Kaspersky Industrial Cybersecurity Conference 2019


+2.000 Members worldwide

All actors involved in Cybersecurity in Industrial Environments

End users

Public bodies

Device manufacturers

Engineering

Integrators

Cybersecurity providers

CCI Coordinators

North America


José Torres


Patrick Miller

Centre America


Raúl Rivera

South America


Andrea Parada


Claudio Caracciolo


Diego Andrés Zuluaga


Fernando Guerrero


Ernesto Landa


Gabriel Bergel


Hernán Vázquez


Jesus Peña


Jorge Abanto


Juan Carlos Gómez


Marcelo Branquinho


Mateo Martinez


Nora Alzua


Santiago Vazquez

CCI Coordinators

Europe


Belén Pérez


Dr. John McCarthy


Edorta Echave


Javier Cao


Jesús Mérida


Joan Figueras


José Luis Jiménez


José Valiente


Juan Miguel Pulpillo


Laurent Pelud


Marcin Dudek


Óscar Bou


Piotr Jasinski


Stephen Smith


Susana Asensio


Vicente Asensi

Asia


Anton Shipulin


Ayhan Gücüyener


Can Demiral

Middle East


Ignacio Paredes


Ayman Al-Issa

CCI Experts

- Critical Infrastructure:

Santiago G. Gonzalez

- Cybersecurity Management Systems:

José Valiente

Samuel Linares

- Forensic Analysis Expert:

Javier Pagès

Joan Figueras

Gustavo Presman

- ICS Threat Intelligence:

Robert M. Lee

- Industrial Hacking:

Claudio Caracciolo

Ignacio Paredes

Silvia Villanueva

- Industrial Security:

Arturo Trujillo

CCI Experts

- Industrial Systems:

David Marco

Hector Puyosa

- Industrial Networks:

Ignacio Álvarez

- Legal Compliance:

Paloma Llaneza

- Manufacturing Execution Systems:

Antonio Rodríguez U.

- Physical Security:

Miguel Merino

- Resilience and Continuity:

Eduardo Di Monte

- Security and Privacy Management Systems:

Carlos Asún


21
studies


11
countries
21
studies


11
countries
21
studies
+650
industrial
organizations


+650
industrial
organizations
North
Americ
a
Central
& South
Americ
a
21
studies
Europe
11
countries

Contrasted gaps

Contrasted gaps

Common Solutions in a Global OT Environment

UNAWARENESS, LACK OF TRAINING & QUALIFICATION

INDUSTRIAL CYBERSECURITY RESPONSIBLE

CIBERSECURITY IN NEW PROYECTS

INCIDENT INFORMATION SHARING

REGULATIONS, NORMS & STANDARDS

UNAWARENESS, LACK OF TRAINING & QUALIFICATION


?
ASSETS

IF YOU DON'T KNOW WHAT YOU'VE GOT...

HOW CAN YOU PROTECT IT?


NO
DIAGNOSIS

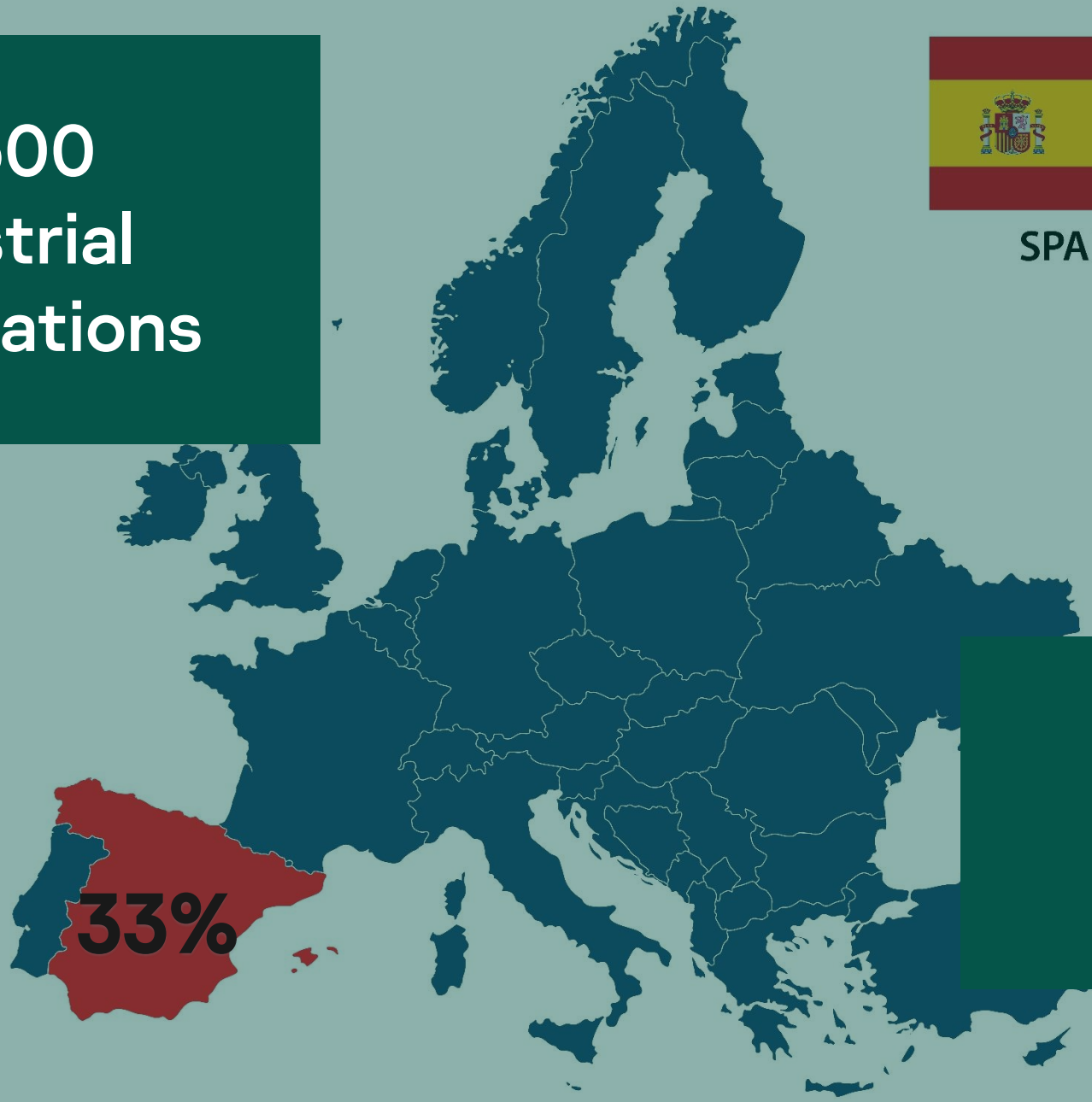
Our participants

217
organizations

33%

Have not carry out a risk assessment

63.500
Industrial
organizations

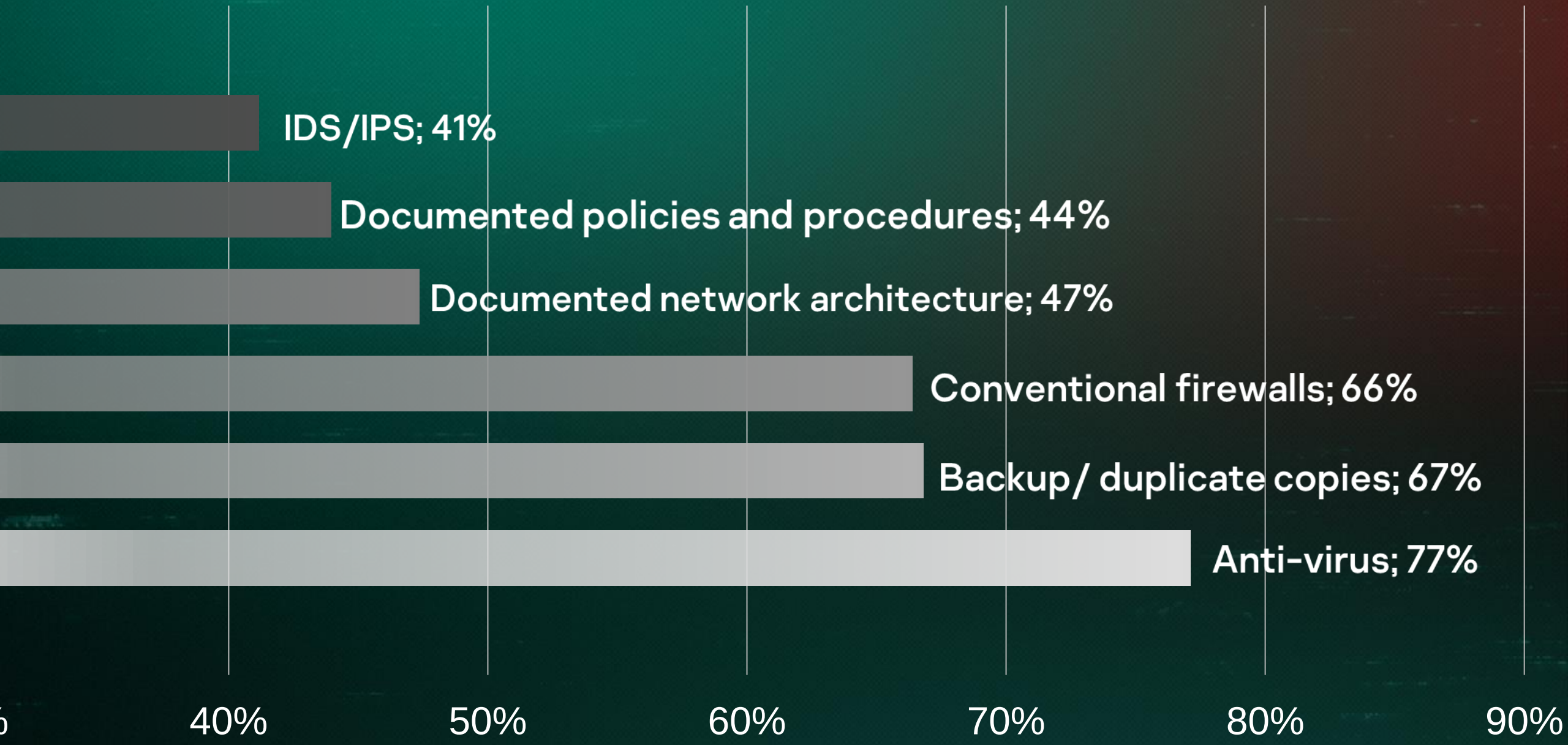


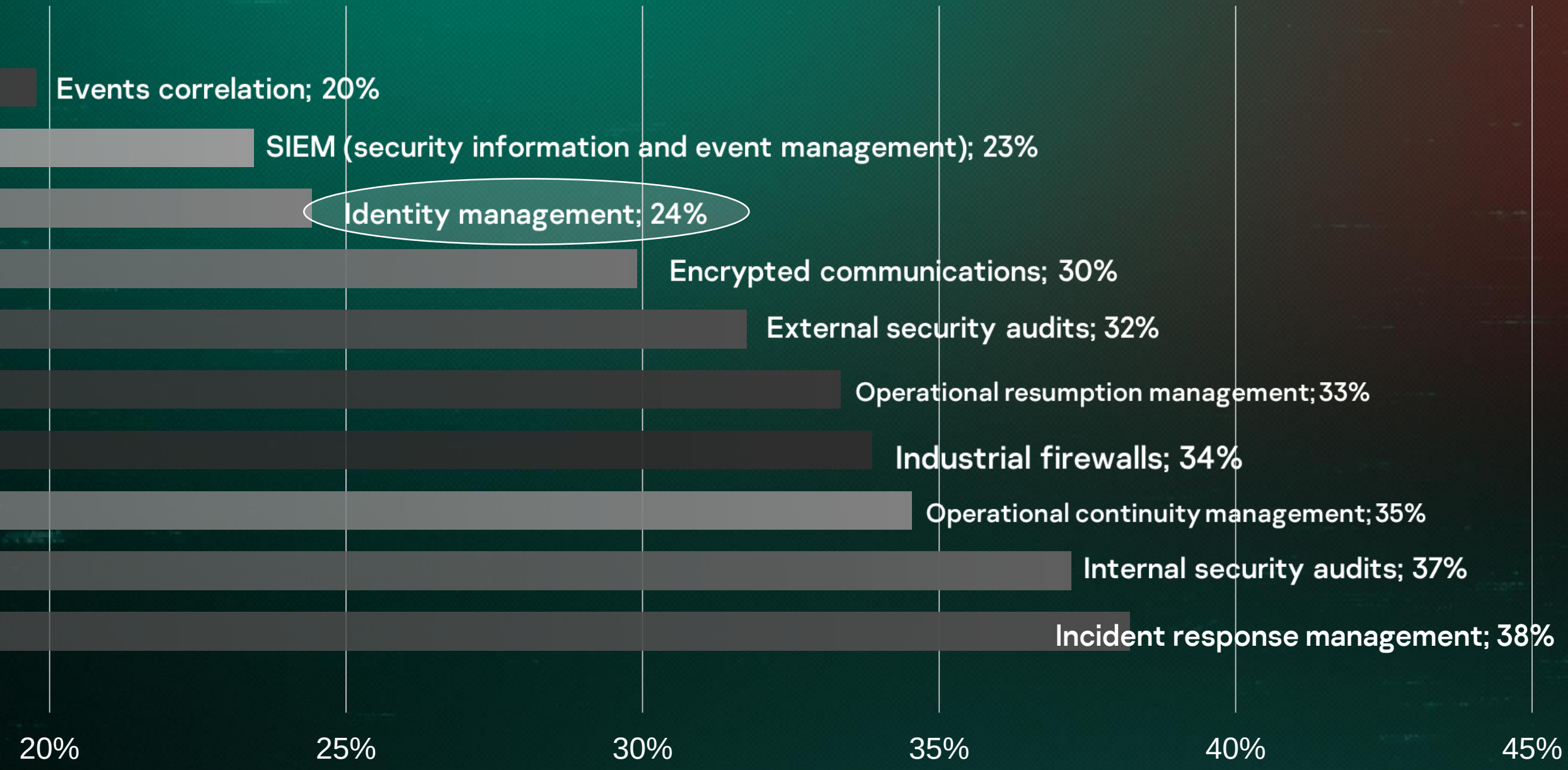
SPAIN

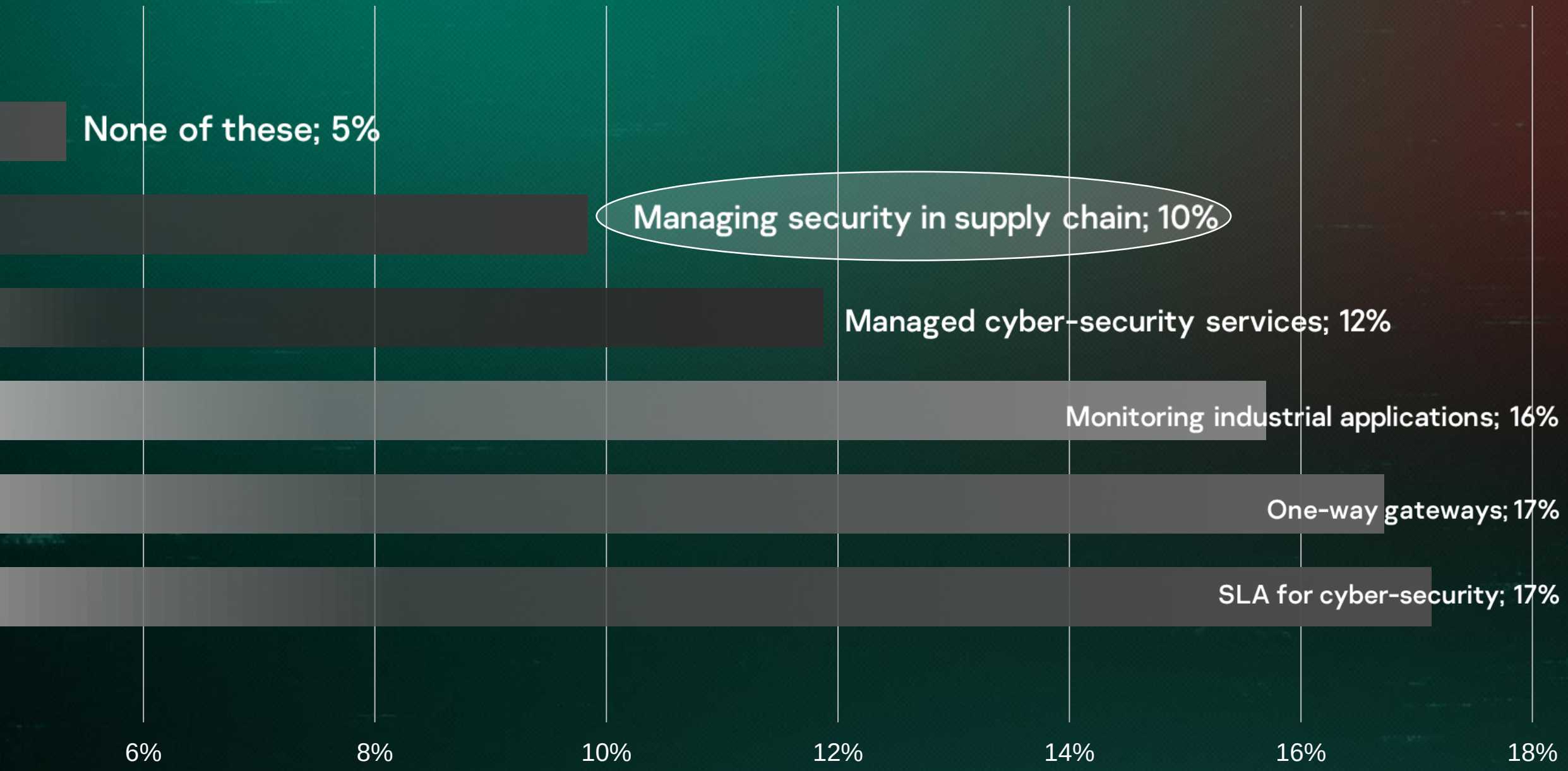
700.000
employees


We have assessed some organisational aspects (policies, procedures)
37%
We have undertaken a technical assessment (segmentation, intruder tests)
30%
We have carried out an assessment based on current standards (ISA99, LPCI or other)
16%
ISO 27005
15%
Other
11%
MAGERIT
3%

VULNERABILITIES


IDS/IPS; 41%
Documented policies and procedures; 44%
Documented network architecture; 47%
Conventional firewalls; 66%
Backup/ duplicate copies; 67%
Anti-virus; 77%
40%
50%
60%
70%
80%
90%


Events correlation; 20%
SIEM (security information and event management); 23%
Identity management; 24%
Encrypted communications; 30%
External security audits; 32%
Operational resumption management; 33%
Industrial firewalls; 34%
Operational continuity management; 35%
Internal security audits; 37%
Incident response management; 38%
20%
25%
30%
35%
40%
45%


None of these; 5%
Managing security in supply chain; 10%
Managed cyber-security services; 12%
Monitoring industrial applications; 16%
One-way gateways; 17%
SLA for cyber-security; 17%
6%
8%
10%
12%
14%
16%
18%

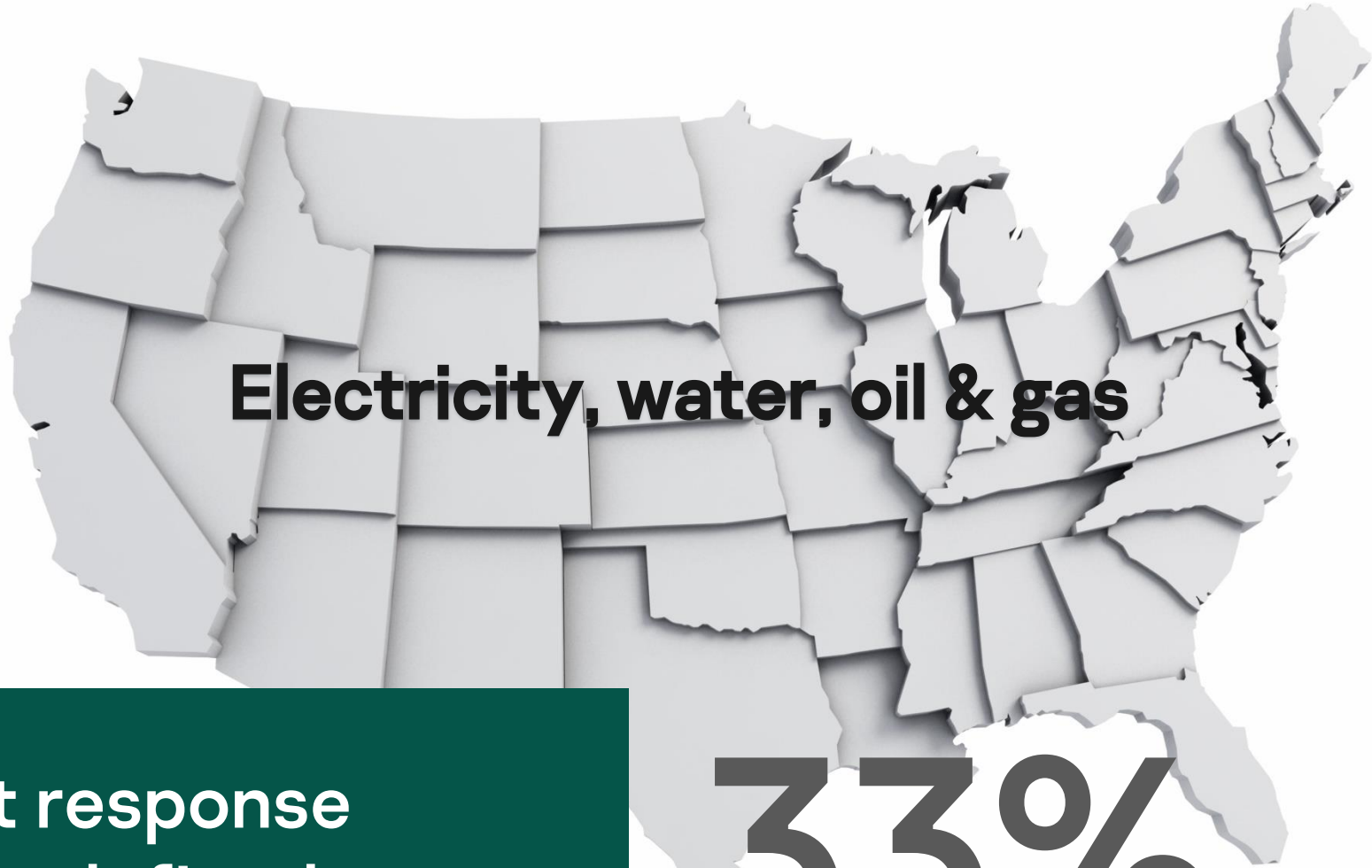

NO
INTEGRATION

30%

Have not defined an incident procedure

A cyber incident response process has been defined, implemented and tested

50%



A cyber incident response process is being defined

33%

Cyber incident response is reactive

17%

17%

CYBER INCIDENT RESPONSE IS REACTIVE

8.529
Infrastructures
215.739
Employees

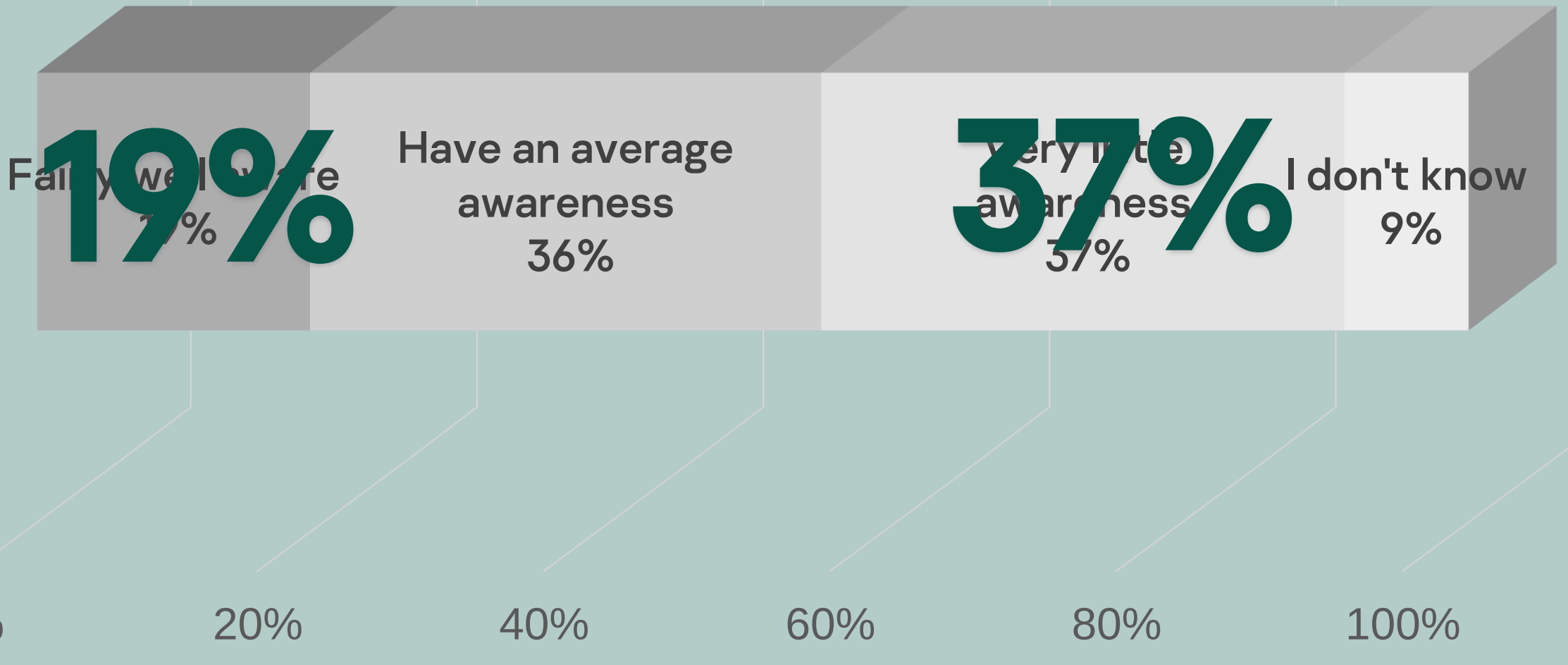
LACK OF TRAINING & QUALIFICATION

RISK PERCEPTION

LACK OF TRAINING & QUALIFICATION

RISK PERCEPTION

SUPPORT

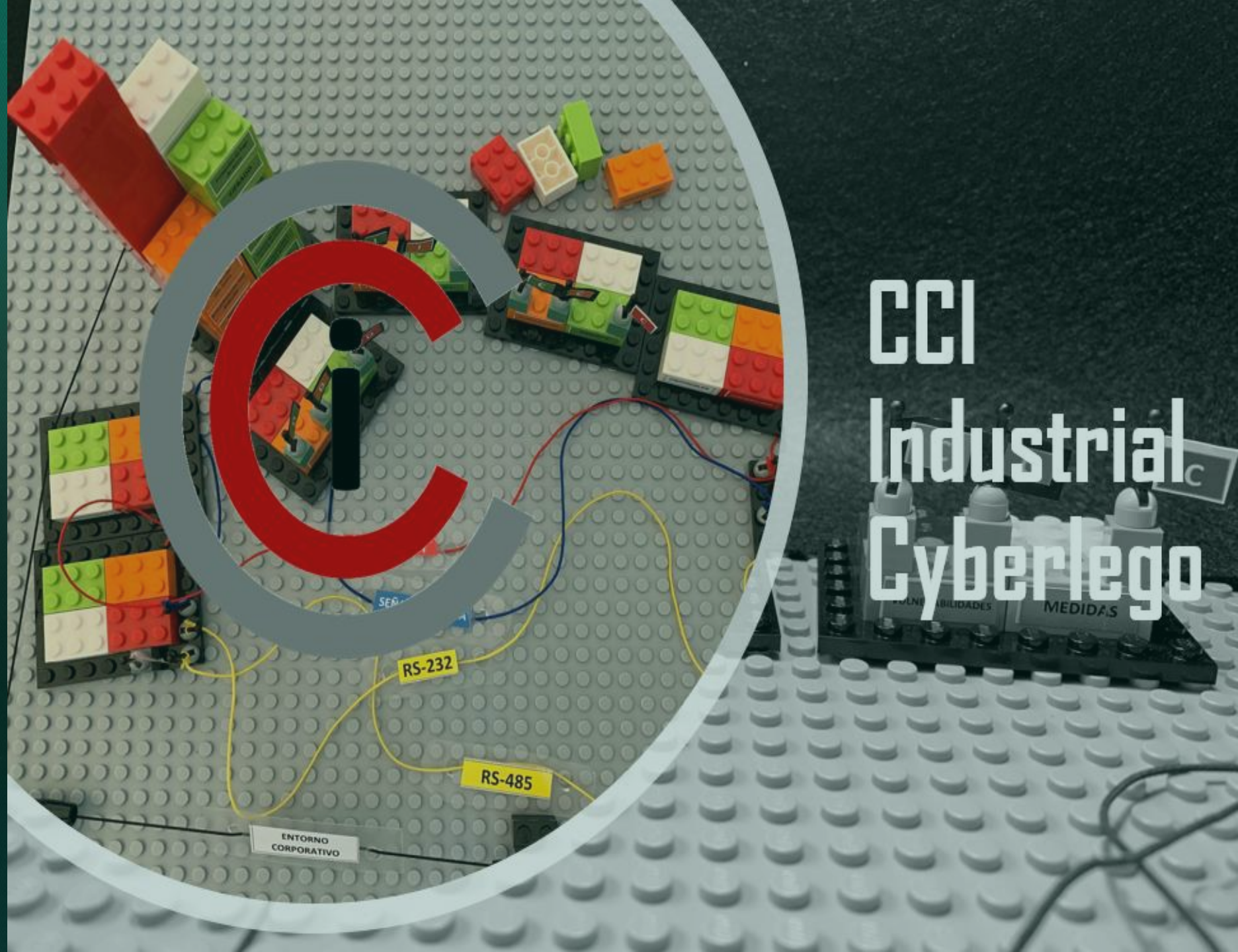

19%
Have an average awareness
36%
37%
I don't know
9%
0%
20%
40%
60%
80%
100%

LACK OF TRAINING & QUALIFICATION

- RISK PERCEPTION
- SUPPORT
- REQUIREMENTS
- CRITICAL CAPACITY
- SUPPLY

PLEASE,

work on awareness, training, and qualifications




BUSINESS LAW

CYBERSECURITY IN NEW PROJECTS

IMPACT

- Performance
- Deployment
- Budget

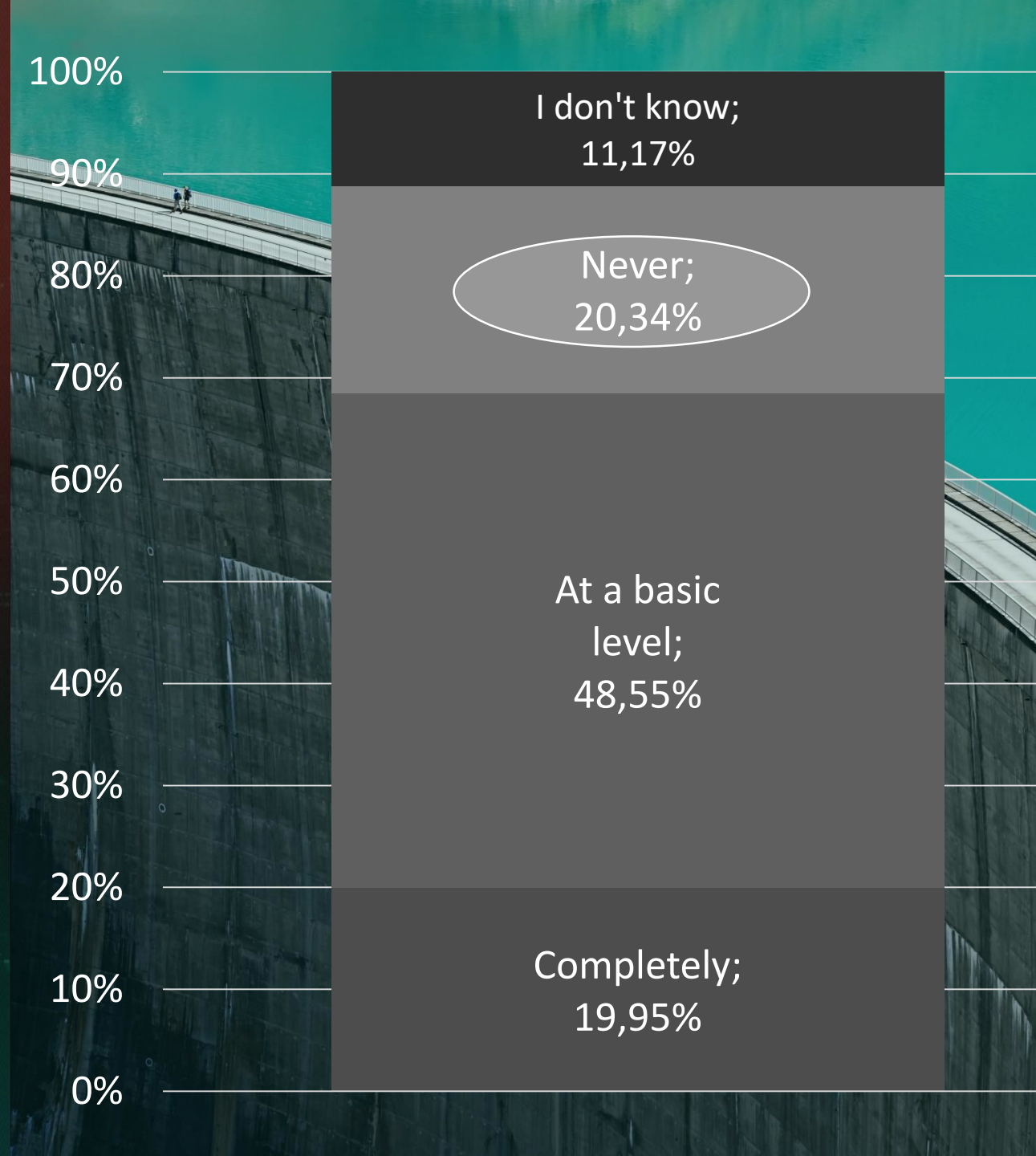
EXISTANCE

- Industrial technology
- Providers
- Law or standard

VALIDATION

PROFESSIONALS

Design phase requirements



INDUSTRIAL CYBERSECURITY RESPONSIBLE

INDUSTRIAL CYBERSECURITY RESPONSIBLE

WITHOUT THE INDUSTRIAL CYBERSECURITY RESPONSIBLE

LACK OF LEADERSHIP

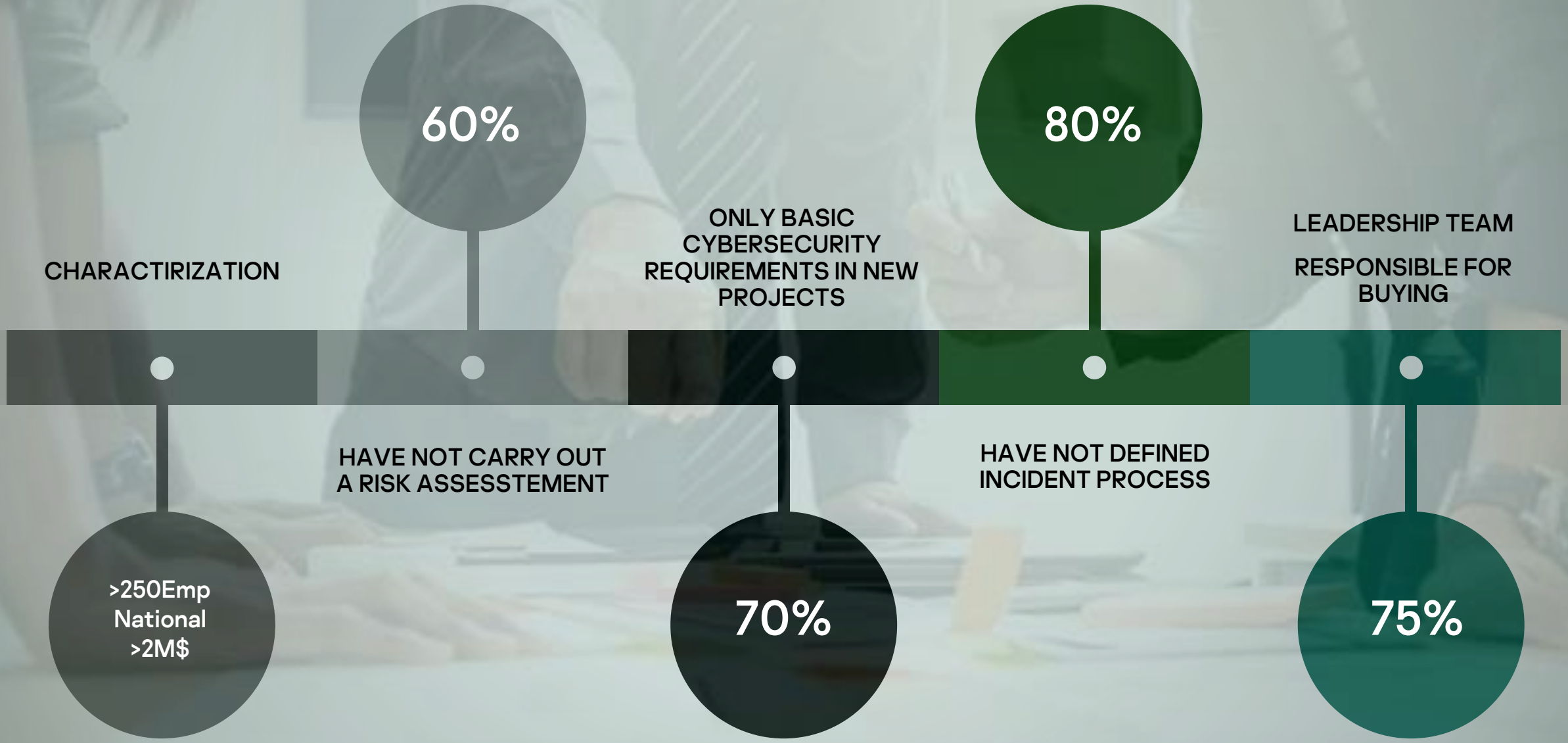
LACK OF SUPPORT

LACK OF STRATEGIC ALIGMENT

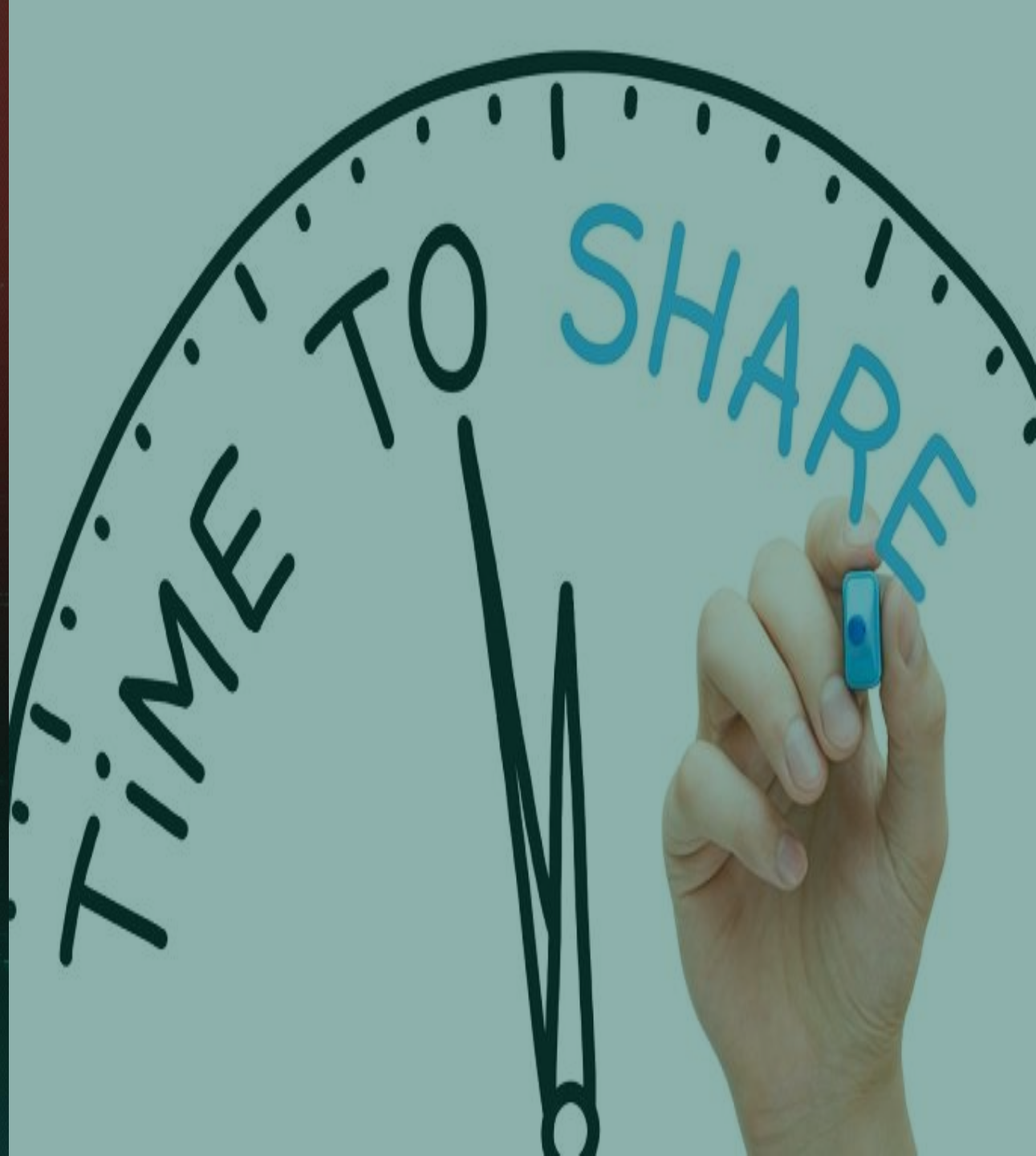
CONSEQUENCES

COMMITMENT

WITHOUT THE INDUSTRIAL CYBERSECURITY RESPONSIBLE



INCIDENT INFORMATION SHARING



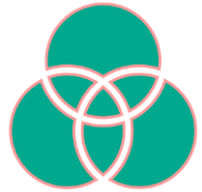
We all are in the same boat…

Incident notification systems

- Incident notification systems implemented by the states
- Teams need also to get prepare

Cybersecurity exercises

- Attacker & Defense point of view
- Theory and reality are not always the same



Sharing Platform of Industrial Cybersecurity Incident Information

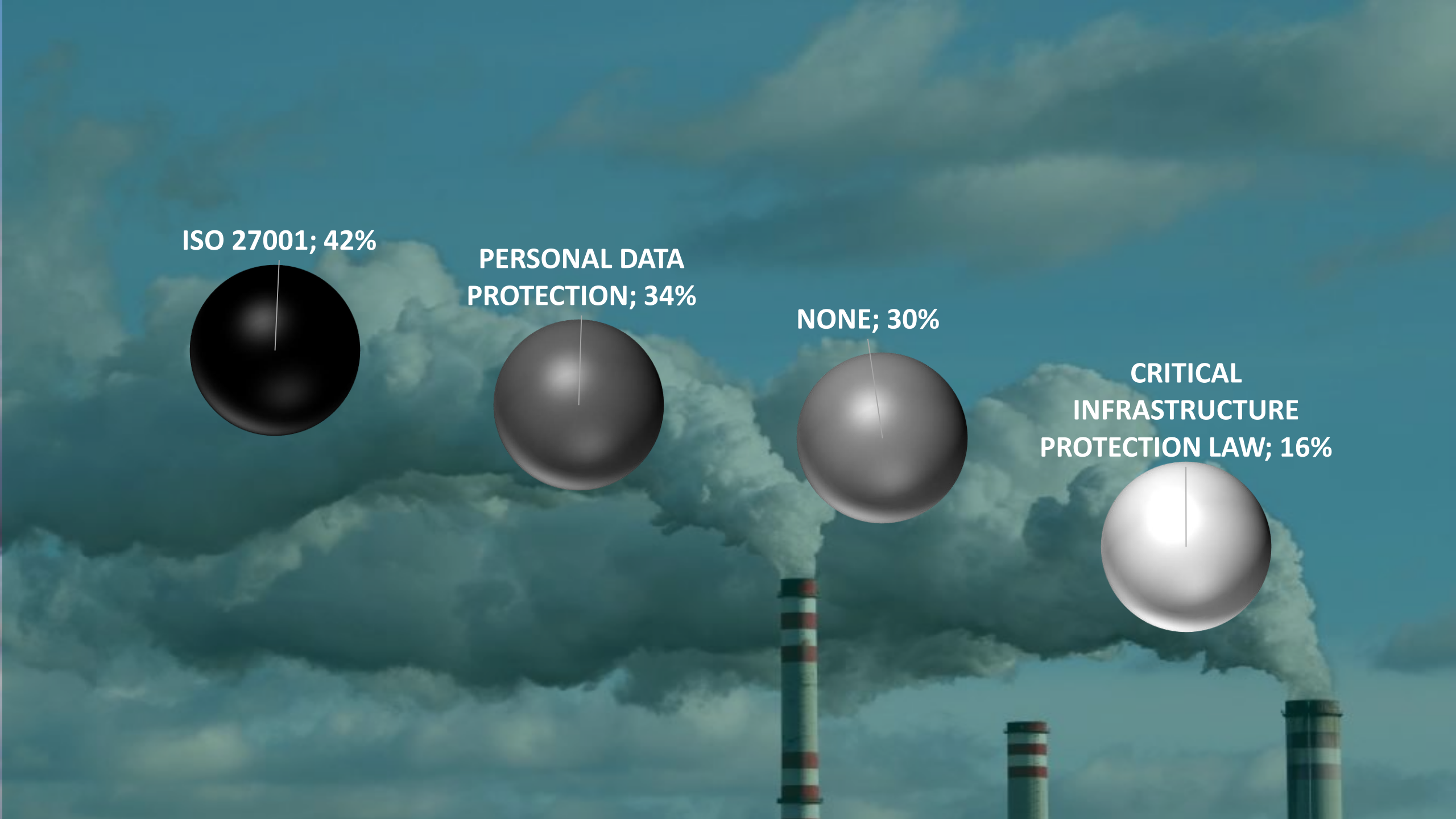
- Incident scenario
- Incident full characterization
- Incident treatment
- **EMPOWERMENT TEAMS**

REGULATIONS, NORMS & STANDARDS

Do not start the house from the roof

30%

DO NOT USE ANY NORMS & STANDARDS


ISO 27001; 42%
PERSONAL DATA PROTECTION; 34%
NONE; 30%
CRITICAL INFRASTRUCTURE PROTECTION LAW; 16%

But they are not enough

Disinformation
&
Uncertainty

Proactive measures

Control actions based on
analisys of malicious activity

Reactive measures

Learning algorithms
&
Model training

Anticipative measures

Initiatives

CCI INITIATIVES

UNAWARENESS, LACK OF TRAINING & QUALIFICATION

EVENTS & TEAMS & INDUSTRIAL CYBERSECURITY SCHOOL

INDUSTRIAL CYBERSECURITY RESPONSIBLE

GUIDE & CREDENTIALS & INDUSTRIAL CYBERSECURITY SCHOOL

CIBERSECURITY IN NEW PROYECTS

TECHNICAL PLATFORM OF INDUSTRIAL CYBERSECURITY REQUIREMENTS

INCIDENT INFORMATION SHARING

INDUSTRIAL CYBERSECURITY INCIDENT INFORMATION SHARING PLATFORM

REGULATIONS, NORMS & STANDARDS

ICMS, INDUSTRIAL CYBERSECURITY SCHOOL, EUROPEAN LAW GUIDE

Kaspersky Industrial CyberSecurity

PRODUCTS

Industrial Endpoint Protection

KICS for Nodes

Industrial Anomaly and Breach Detection

KICS for Networks

Centralized security management

Kaspersky Security Center

SERVICES

Training and awareness

Kaspersky® Security Awareness

Kaspersky® Security Trainings

Expert services and intelligence

Kaspersky® Security Assessment

Kaspersky® Incident Response

Kaspersky® Threat Intelligence

PLEASE,

BUILD TEAM

THAT, NEVER FAILS

Cybersecurity grows, as it grows the team trust

THAT'S ALL
THANK YOU
;-)

www.cci-es.org

susana.asensio@cci-es.org