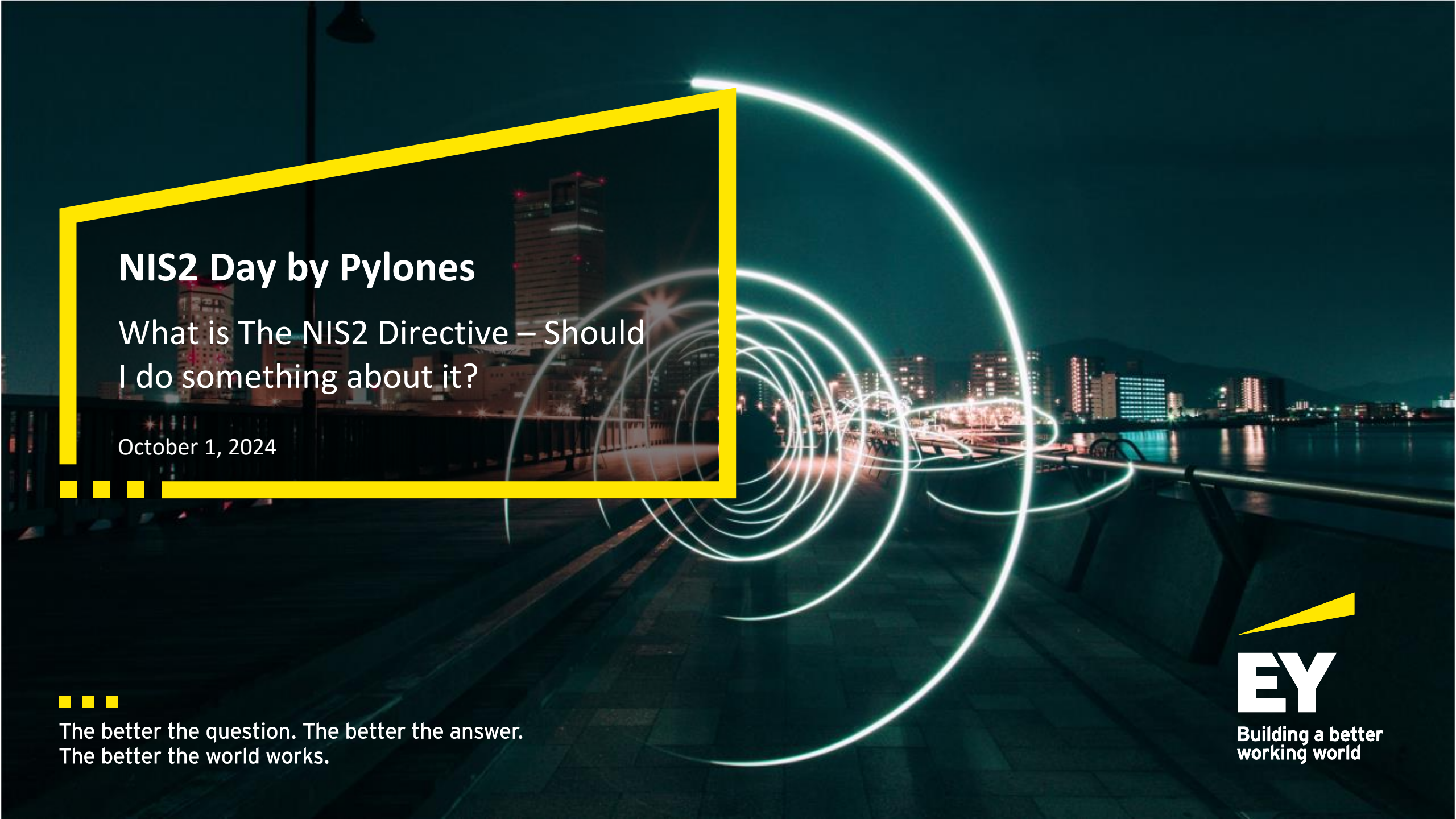


NIS2 Day by Pylones

What is The NIS2 Directive – Should I do something about it?

October 1, 2024

The better the question. The better the answer.
The better the world works.

Building a better working world

With you today

Vasilis Christopoulos

Director @ EY

Technology Consulting | Cybersecurity

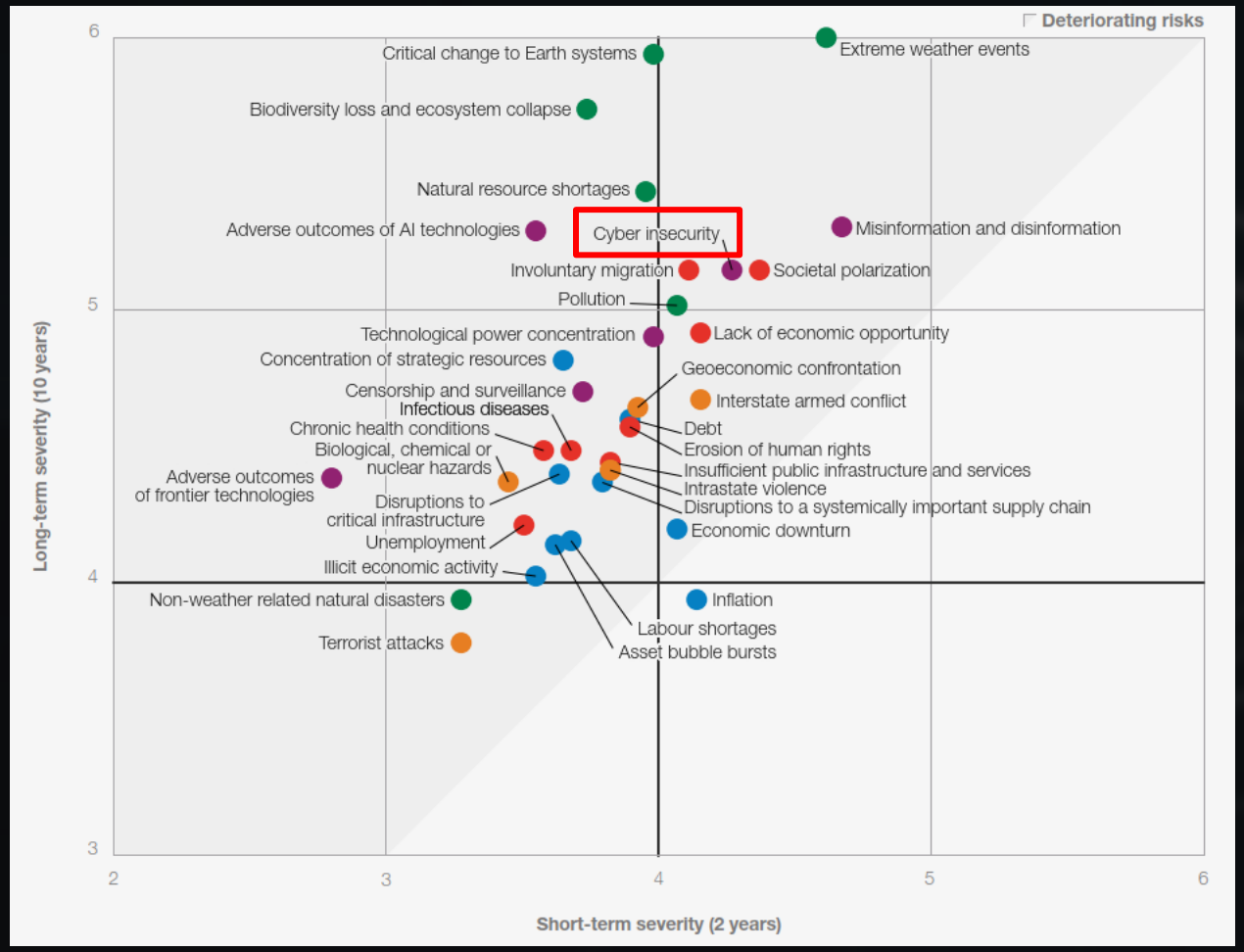
Vasilis.christopoulos@gr.ey.com

#whoami

- ✓ Specializing in Cyber, Data Protection, and Microsoft Cloud Security
- ✓ Joined EY in 2019
- ✓ Driving EY's EMEIA Microsoft Cloud Security Hub in Athens
- ✓ BSc degree in Informatics, MSc degree in Information System from Athens University of Economic and Business
- ✓ CISSP, CISM, CDPSE, CIPM, ISO27001LA, ISO22301LA
- ✓ TAE KWON DO Certified Instructor

Setting the scene

Cybersecurity is now considered a top risk while being at the forefront of global developments



World Economic Forum: Global Risks Report 2024 - Relative severity of risks over a 2 and 10-year period

+ Digital Single Market

The regulatory landscape is becoming broader and more complex

Timeline for adoption of different regulations in the EU (non-exhaustive)

August 2016

NIS

Requirements for cybersecurity critical sectors

May 2018

GDPR

Regulation for protection of personal data

February 2024

Digital Services Act

Rules to protect the rights of digital services users

March 2024

Cyber Resilience Act (CRA)

Requirements for products/services with digital elements

January 2025

DORA

Requirements for cybersecurity in the financial sector

October 2024

Critical Entities Resilience (CER)

Rules for ensuring the resilience of critical entities

October 2024

NIS2

Requirements for cybersecurity in critical sectors

March 2024

AI Act

Requirements for Artificial Intelligence (AI) applications

Transition from NIS to NIS2

NIS2 looks to expand the goals and scope of NIS

Goals set out by NIS Directive (2016)

To improve the overall level of cybersecurity in EU

To enhance the security of critical infrastructure

To promote cooperation among EU Member States

To establish a culture of risk management

To ensure a common level of preparedness

… The NIS Directive fell short of expectations …

Renewed goals set out by NIS2 Directive (2022)

To cover a larger share of the economy and society by including more sectors

To strengthen specific domains, such as resilience and security in the supply chain

To increase requirements and reporting obligations

To harmonize penalty and supervision regimes

NIS2 in-scope entities

From OESs & DSPs to Essential & Important entities

Essential Entities

- Energy
- Transport
- Financial Market Infr.
- Banking
- Healthcare
- Providers of public electronic comm. networks & services
- Waste Water
- Digital Infrastructure
- Public Administration
- Drinking Water
- Space

Stricter supervisory and penalty regimes including:

- ✓ **Ex-ante and ex-post supervision**, regular, targeted and ad-hoc audits etc.
- ✓ A maximum of at least **10,000,000 EUR** or up to **2%** of the total worldwide annual turnover (whichever is higher).

Important Entities

- Digital providers
- Postal & courier services
- Waste mgmt.
- Chemicals
- Manufacture
- Food
- Research

Lighter supervisory and penalty regimes including:

- ✓ **Ex-post supervision**, targeted audits etc.
- ✓ A maximum of at least **7,000,000 EUR** or up to **1,4%** of the total worldwide annual turnover (whichever is higher).

Cybersecurity risk management is a main focus of NIS2

NIS2 imposes new cybersecurity risk management requirements for in-scope entities

Risk analysis & information system security

Incident handling

Business continuity

Supply chain security

Security in system acquisition, development and maintenance

*Essential and Important entities must take **appropriate** and **proportional technical, operational and organizational measures** to manage the risks posed to the systems which underpin their services.*

Cyber hygiene practices and cybersecurity training

Cryptography & encryption policies

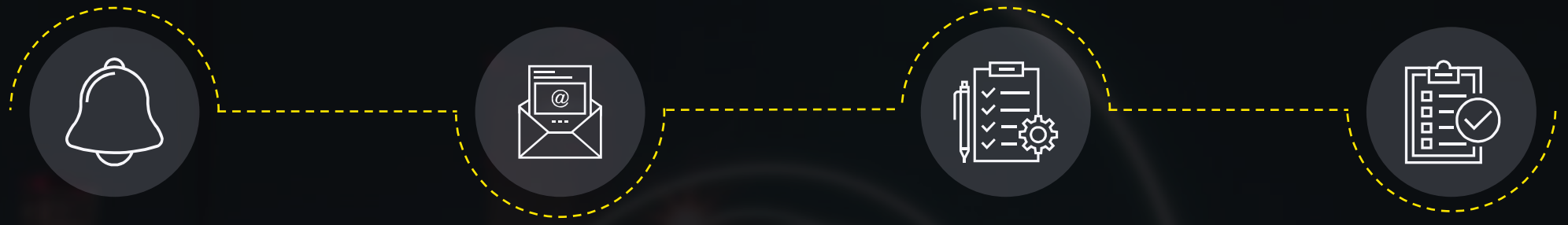
HR security, access control & asset management

MFA and continuous authentication solutions

Policies & procedures to assess risk management measures effectiveness

Incident reporting obligations become much stricter under NIS2

A phased notification obligation to CSIRT / competent Authorities for incidents with significant impacts



Early Warning

…within **24 hours** of becoming aware of a significant incident*

Official Notification

…within **72 hours** providing update on the early warning along with an incident assessment

Intermediate Report

…upon request, indicating a **status update** on the incident handling progress

Final Report

…no later than **1 month** after the submission of the official notification

Under Article 23 (3), an incident shall be considered to be significant if:

- ✓ It has caused or is capable of causing **severe operational disruption** of the services or financial loss for the organization;
- ✓ It has affected or is capable of affecting other natural or legal persons by causing **considerable material or non-material damage**.

Senior management involvement is at the forefront of NIS2 compliance

NIS2 enhances senior management responsibilities over cybersecurity risk management

Key Responsibilities of Important & Essential Entities Management Bodies

Approve the adequacy of cybersecurity risk management measures

Supervise the implementation of the risk management measures;

Follow training relevant to cybersecurity risk management

Ensure relevant training is provided to employees on a regular basis

Be accountable for cases of non-compliance

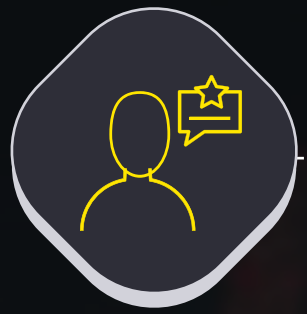
Failure by management to comply with NIS2 requirements could result in:

- Liability
- Temporary bans
- Administrative fines

…as provided for in the implementing national legislation

Key challenges posed by NIS2 that we observe across the market

Achieving consistency within the EU cybersecurity regulatory framework can be quite challenging



Ensuring senior management commitment and accountability

Companies with multinational EU presence need to adjust to the requirements of different implementing acts

Converging different incident notification requirements deriving from different regulations

Management of direct suppliers / service providers relationships to ensure effective management of risks

Next Steps

Key actions to kickstart NIS2 compliance journey

1 Establish a robust cybersecurity risk management framework, infusing supply chain security elements.

2 Enhance incident handling, escalation and reporting capabilities.

3 Safeguard operational resilience and establish proactive crisis management capabilities.

4 Focus on Senior Management engagement and foster a cyber aware culture across the organization.

Thank You!

Q & A

EY | Assurance | Tax | Transactions | Consulting

About EY
EY is a global leader in assurance, tax, transaction and consulting services.
The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity.
Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

About EY's Advisory Services
As better-connected consultants, we help EY clients thrive in the Transformative Age.

Being better-connected lies at the heart of EY Advisory and how we work. It is about bringing together the talents, creativity and experience of the entire organization and alliances. It refers to the way we collaborate with each other, EY clients, market influencers and strategic alliances globally to help the clients realize sustainable results and build a better working world.

We combine a complete understanding of the clients' priorities, such as strategy, digital, technology, analytics, cybersecurity and people, with our competencies in performance improvement, risk and people advisory services.

In an era that presents unprecedented change with limitless opportunity, success in the Transformative Age requires boldness, confidence and leadership to seize the opportunities and rise to the challenges of this new age.

By asking the better questions and finding answers to some of the world's toughest challenges, EY Advisory is helping to build a better working world.

The better the question. The better the answer. The better the world works.

ey.com

EY @EY_Greece EY Greece eygreece EY Greece