www.pwc.com.cy/crimesurvey

# *Global Economic Crime Survey 2016*

*Country summary: Key findings in Cyprus*

# *Adjusting the Lens on Economic Crime*

*Preparation brings opportunity back into focus*

*June 2016*

pwc

# *Agenda*

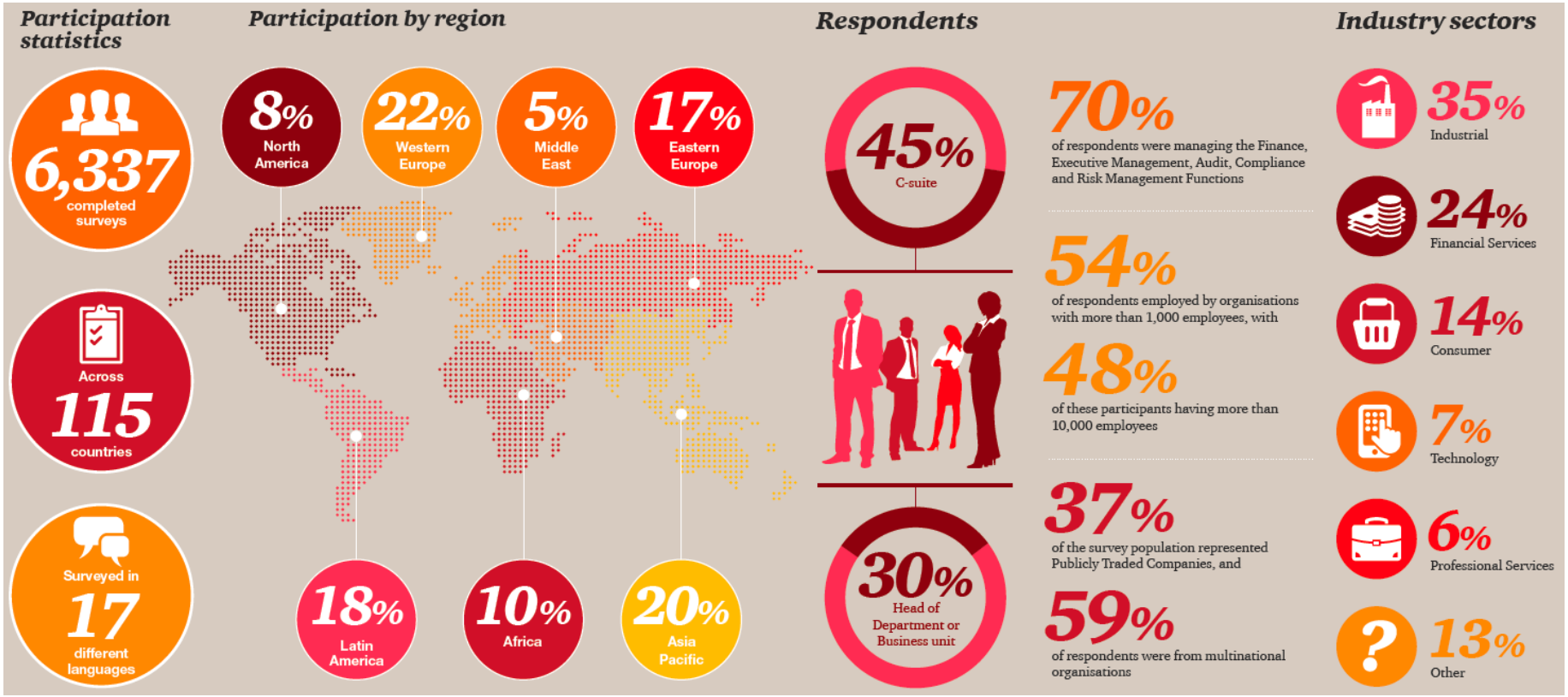
1. Introduction
2. The Big Picture
3. Cybercrime
4. Ethics & Compliance
5. Anti-Money Laundering

# Introduction

# 1

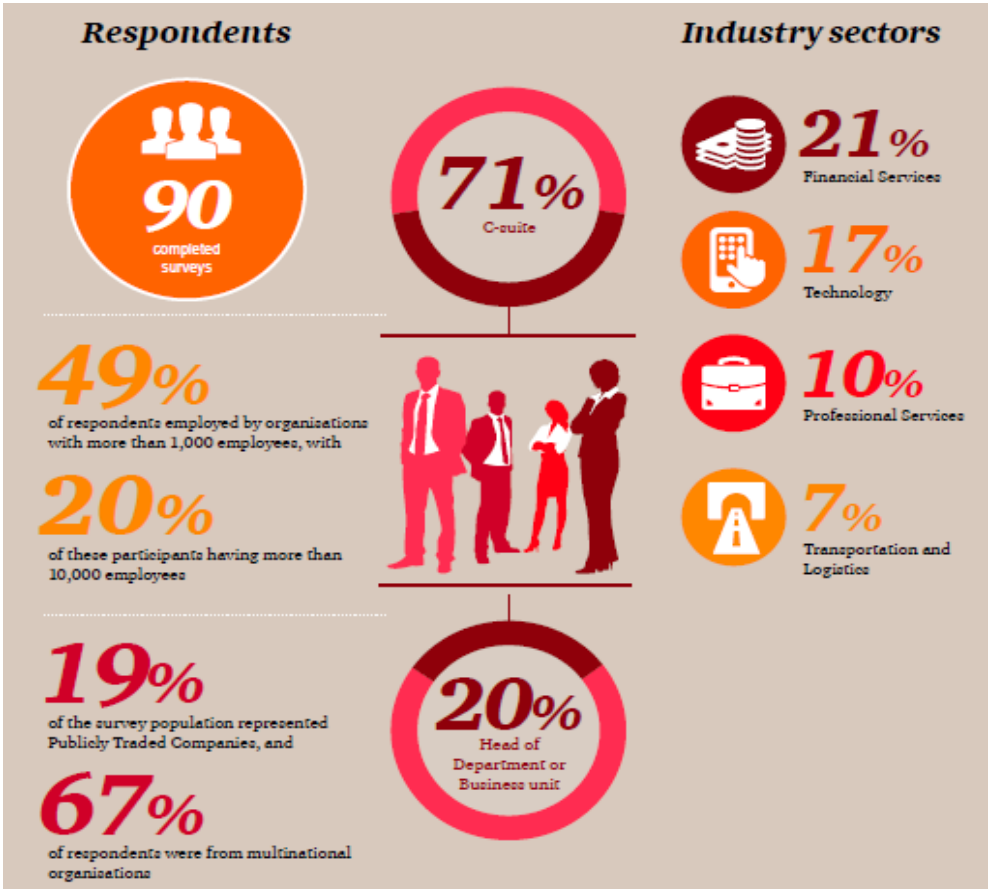
# *Size, scale and depth of the survey*

## *Global*



# *Size, scale and depth of the survey*

## *Cyprus*



## *Economic crime an obstinate threat*
Cyprus is not immune

# *Percentage of responding organisations that experienced economic crime*

*Economic crime is a diversified global issue*

# 27%

## *Need for controls to be embedded in culture*

Threats come from both within and outside organisations

# *2 in 5 organisations have not carried out a fraud risk assessment in the past 24 months*

*Financial damage extending to millions of US dollars in some cases*

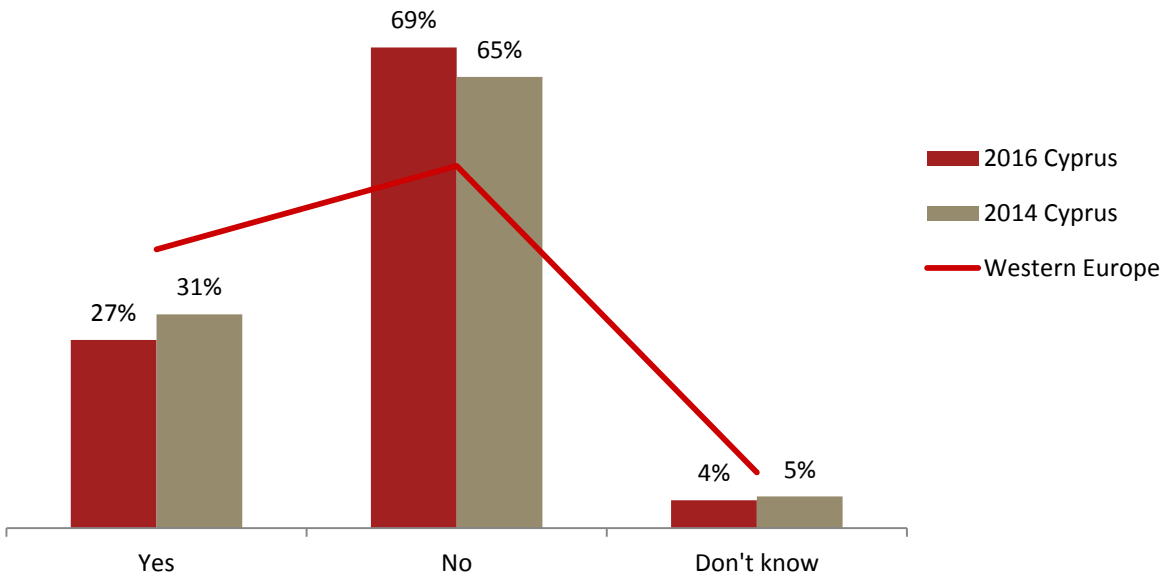
# *42%*

# *The Big Picture*

# 2

# *Economic crime is evolving but preventative measures are lagging behind*

**Has your organisation experienced any economic crime within the last 24 months?**



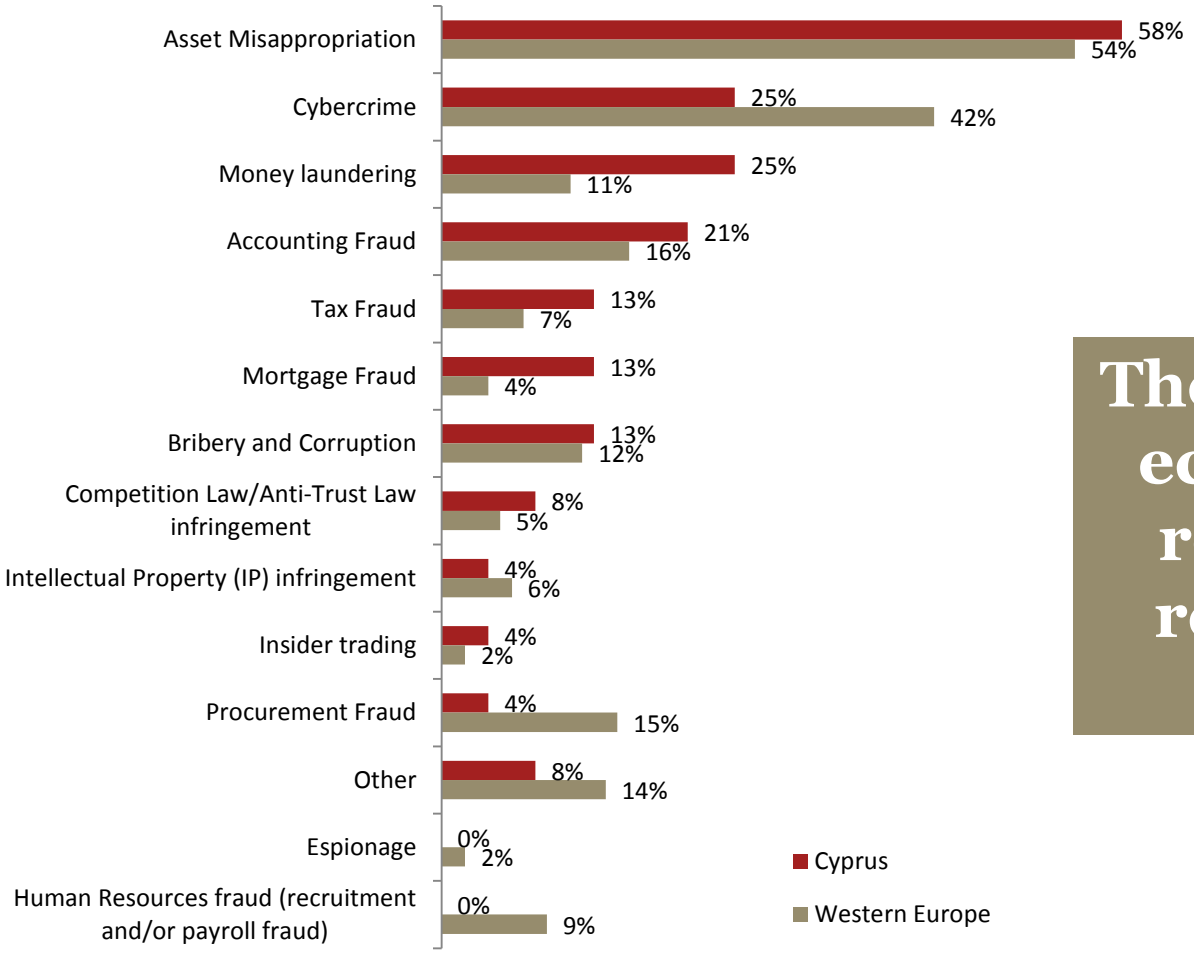

However, a worrying trend may be getting masked: Economic crime may be changing significantly, but detection and control programmes are not keeping up with the pace of change.

# *Top three most commonly reported types of economic crime 2016*


## *Age-old crimes lead, but one pervasive enemy jumps ahead*

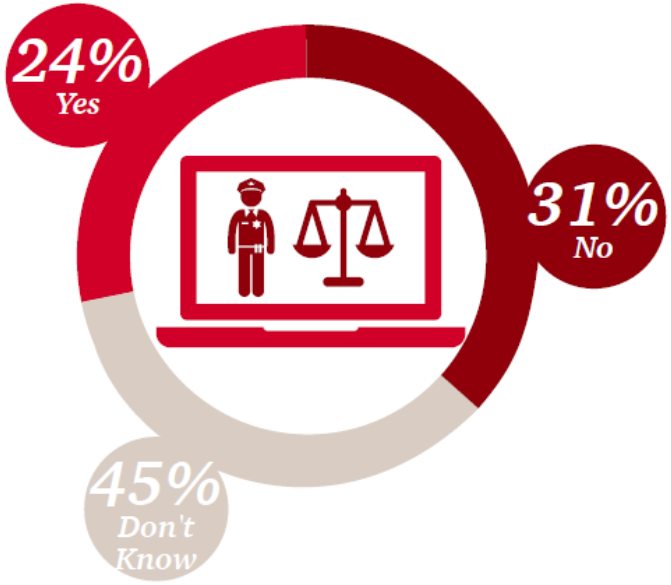
Our findings show that asset misappropriation ranks as the top economic crime, with 58% of respondents suffering from it. This is followed by cybercrime (25%), money laundering (25%) and accounting fraud (21%).

# *Types of economic crime experienced*




**The most pervasive economic crimes reported by our respondents for 2016**

# *Perception of law enforcement*



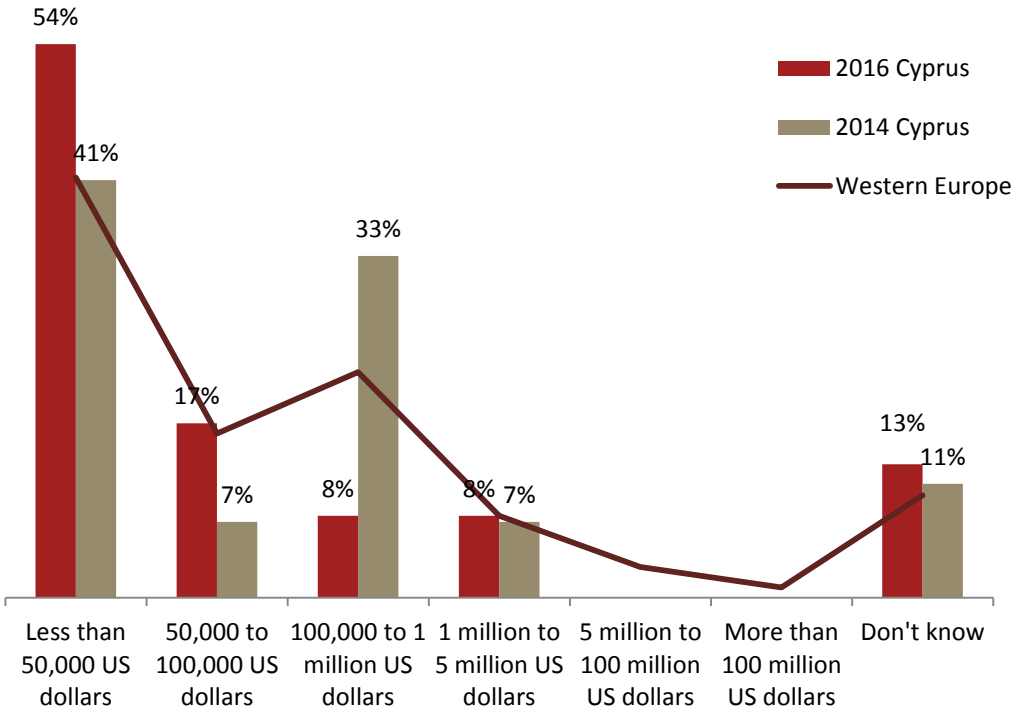

***Do respondents believe local law enforcement agencies are adequately resourced and trained to investigate and prosecute economic crime?***

We asked respondents to give us their views on whether they believe local law enforcement to be adequately resourced and trained to investigate and prosecute economic crime.

Less than a quarter (24%) of our respondents were positive while the majority (45%) did not know what to answer.

# *Financial impact of economic crime*

**Approximate losses through incidents of economic crimes over the last 24 months?**




***Smaller crimes are on the rise***

Increased number of respondents experienced losses of ***$100,000 or less***

**while**

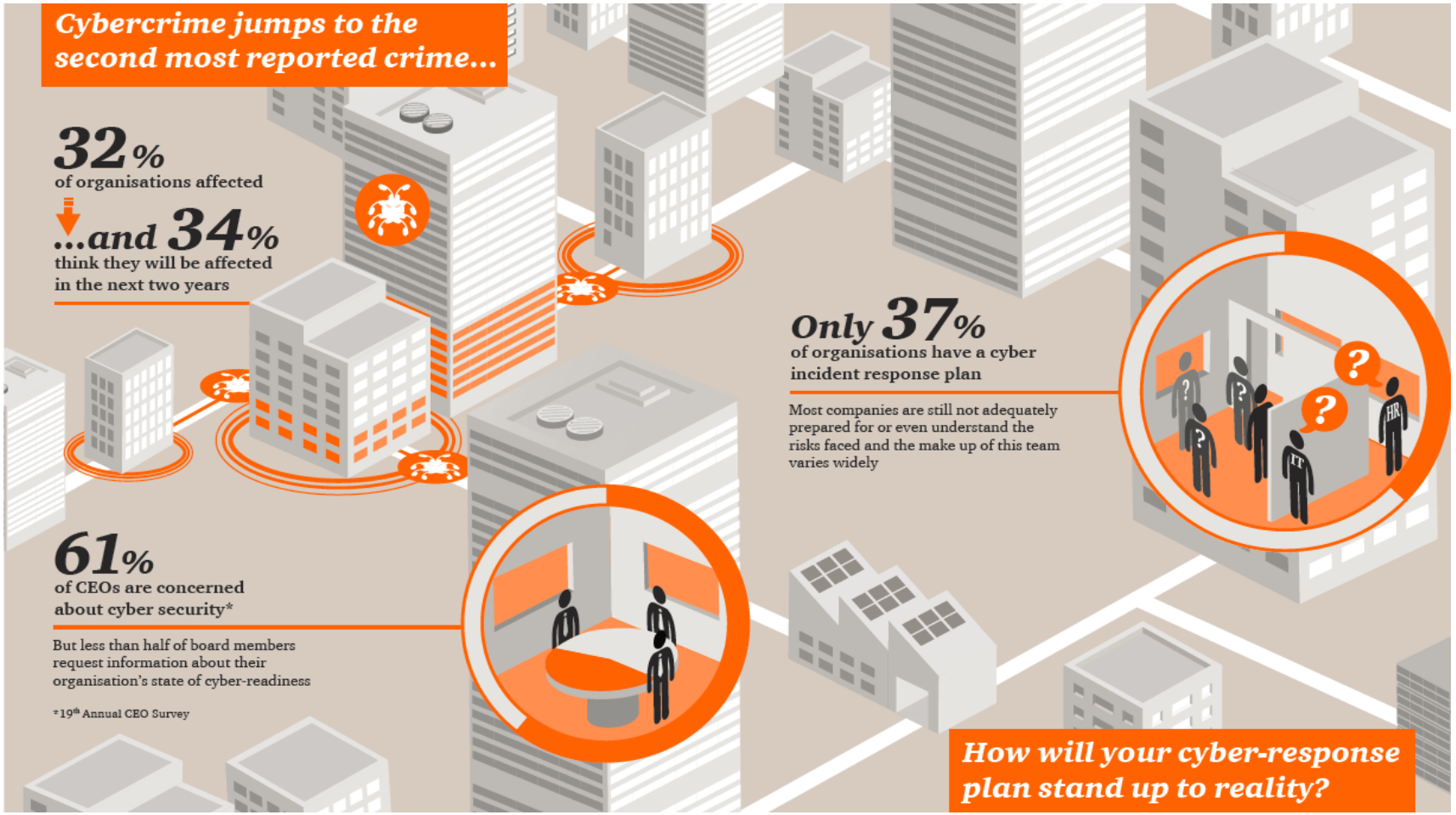
losses of ***more than $100.000 reduced significantly***

These are still substantial sums of money.

# *Cybercrime*

# 3

# *Cybercrime is a boundless threat*
## Global results of the survey



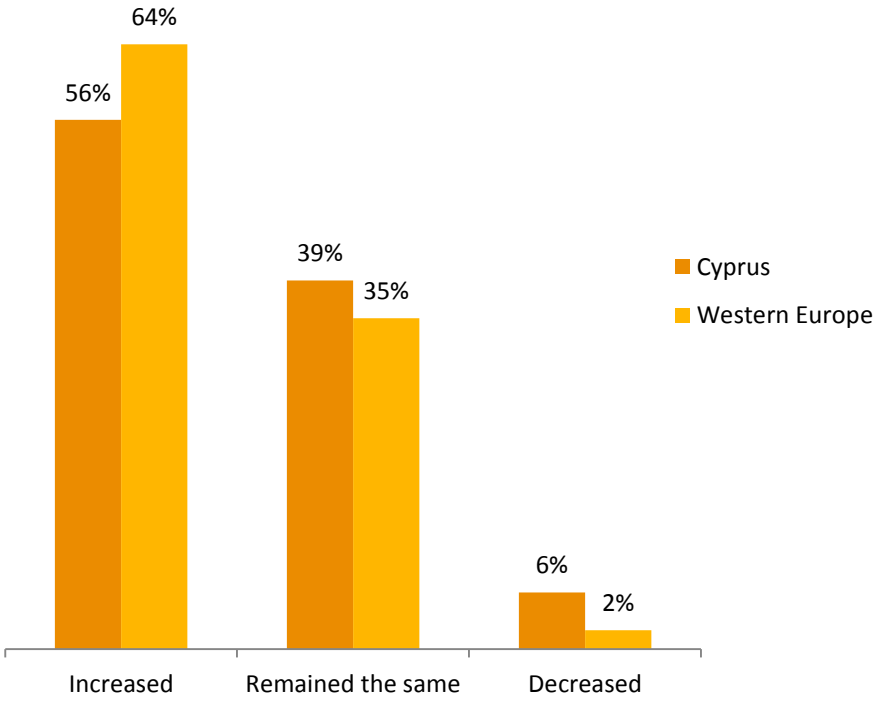
# *Perception of the risk of cybercrime*

## *Ready or not?*

Over half of our survey respondents, ***56%***, see an increased risk of cyber threats, perhaps due to intensifying media coverage.

**But…**

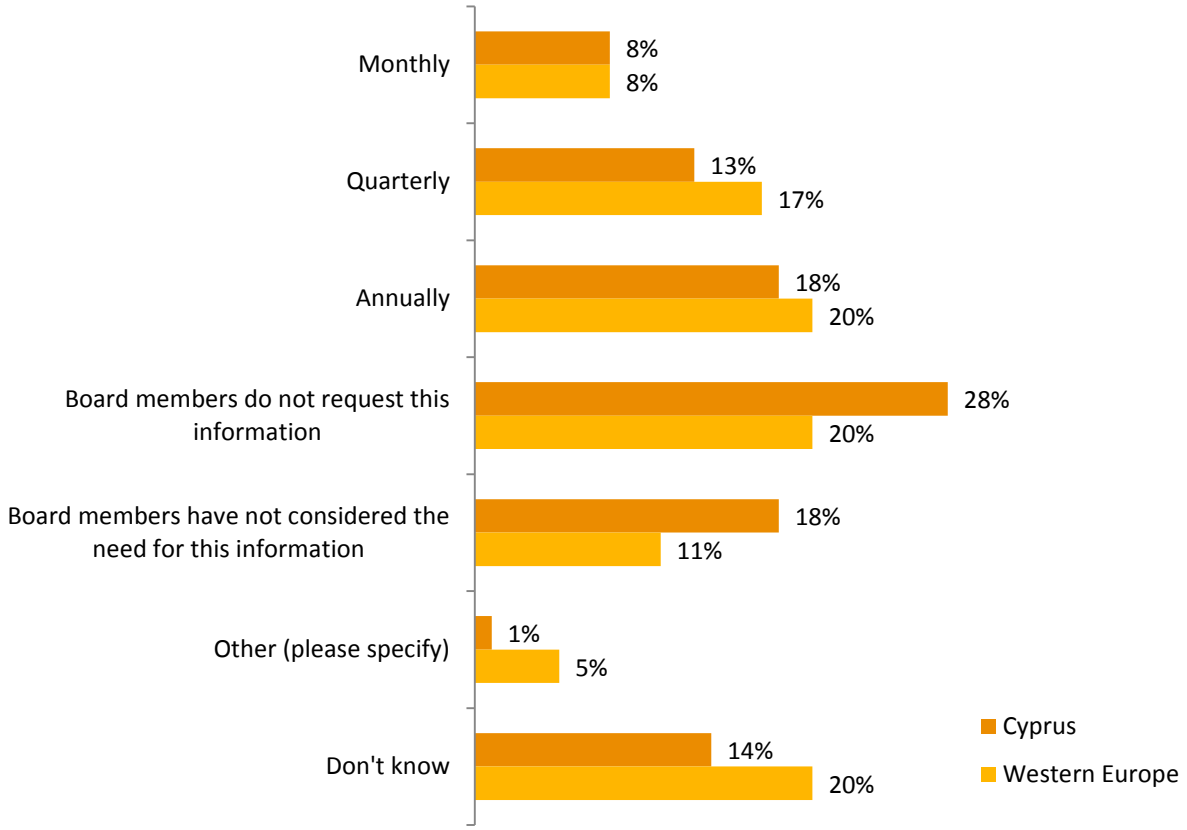
Our survey suggests that companies are nonetheless inadequately prepared to face current cyber threats.



# *Cyber threat vectors: the five categories*

# *Boards are not paying enough attention*

Frequency of requests for information by boards regarding organisations' ability to deal with cyber incidents



# *Cyber Incidence Readiness*

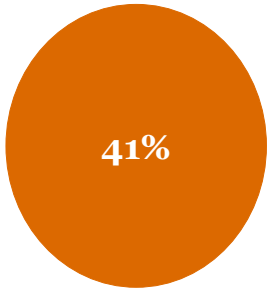
Percentage of respondents with fully operational Incident Response Plans

**32%**

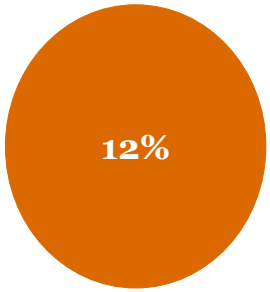
**25%**
don't have a plan
**&**
**27%** of these don't think they need one

# *First Responder Teams*

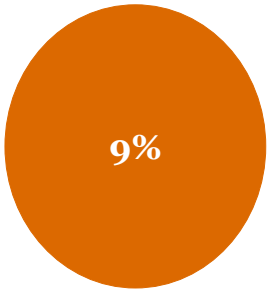
Fully **trained** to act as need arises



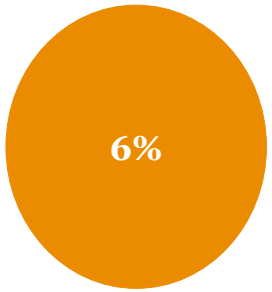

Personnel **yet to be trained**



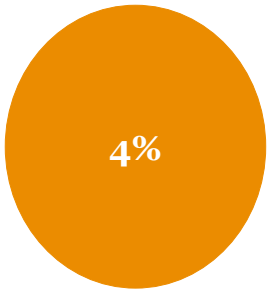

**Outsourced**



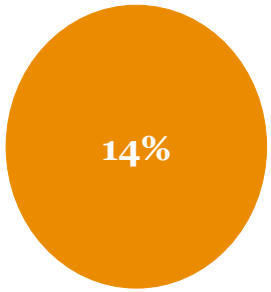

**Have organisations identified First Responder Teams?**




Assessing feasibility of **identifying personnel**




Assessing feasibility of **sourcing an extremal provider**




Organisation feels it **does not need** first responders

# *First Responder Teams*

**IT Security**

70%

**IT staff** (with understanding of entity / organisation IT environment)

61%

**Senior level management**

50%

**Composition of First Responder Teams**

16%

**Attorney** (to provide legal advice)

11%

**Human resources representative**

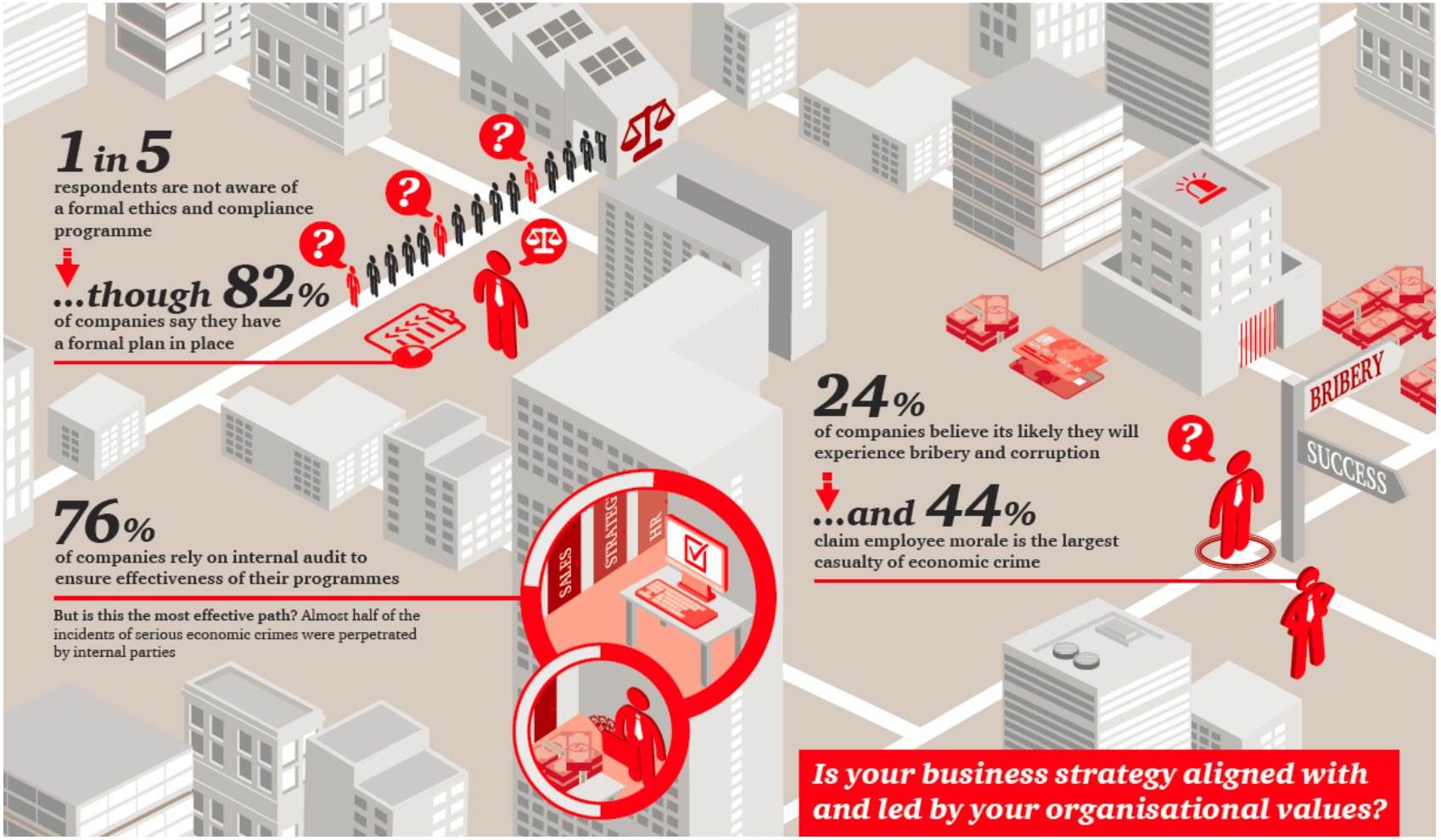
7%

**Digital forensic investigator**

# *Ethics & Compliance*

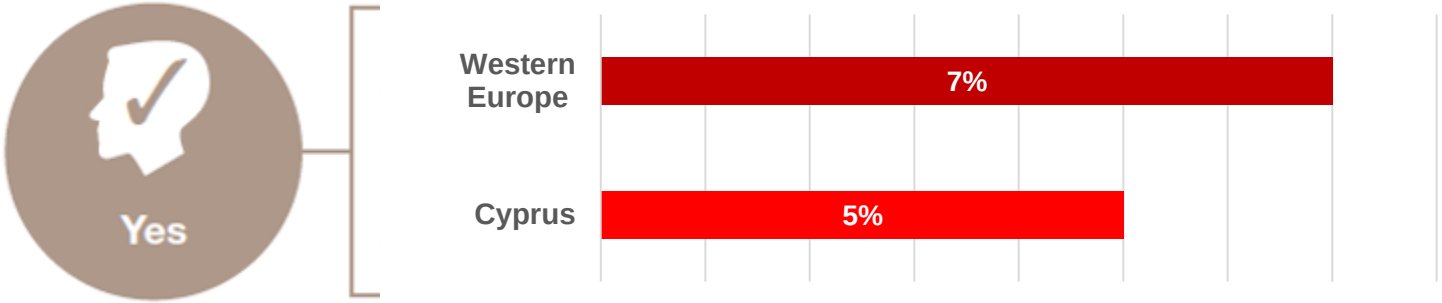
# 4

# *Aligning decision-making with values*
## Global results of the survey



# *Bribery and corruption*

*Percentage of organisations asked to pay a bribe*




***17% of respondents said that they don't know if their organisation was asked to pay a bribe.***

# *Aligning decision-making with values*

A worrying **42%**

of organisations have not carried out a fraud risk assessment in the past 24 months...

...while 8% do not know if they have done so.

Our survey results show that not only is the number of economic crime risks increasing, so too are the **complexity** of those risks and the role that technology plays.

A **risk-based approach** to ethics and compliance – one that begins with a holistic understanding of a company's economic crime risk, and an understanding of where compliance weaknesses are – is a **must-have**.

From that position of clarity, a company can create an effective programme that mitigates those risks.

# *Responsible people want to work for responsible companies*

***7 in 10** of companies say they have a formal plan in place*

***and***

***35%** of respondents say that responsibility lies with Chief Compliance Officer*

**66% of companies rely on internal audit to ensure effectiveness of their programmes…**

**This could be further enhanced by taking more proactive measures like performing a fraud risk assessment, which can reveal the weak spots.**

**Currently only 5% of respondents say they are using other, promising external and internal monitoring approaches**

# *Is your compliance programme fit-for-purpose?*

**4 key areas of focus** for enhancing the effectiveness of ethics and compliance programmes:

**1. People and culture**
Maintaining a values-based programme, measuring and rewarding desired behaviour

**2. Roles and responsibilities**
Ensuring they are correctly aligned with current risks

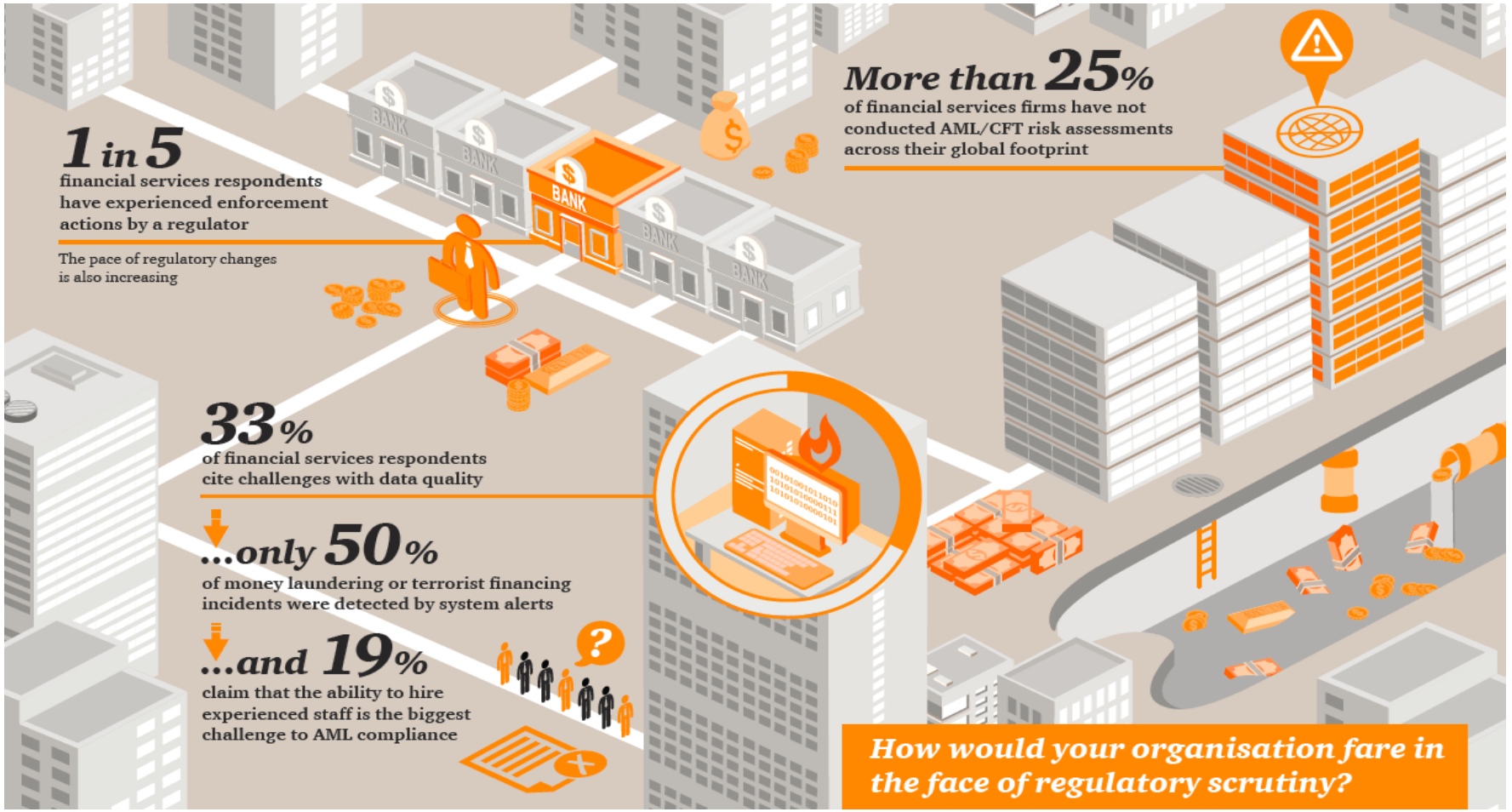
**3. High-risk areas**
Better implementation and testing of the programme in high-risk markets and divisions

**4. Technology**
Better use of detection and prevention tools, including big data analytics

# *Anti-Money Laundering*

# 5

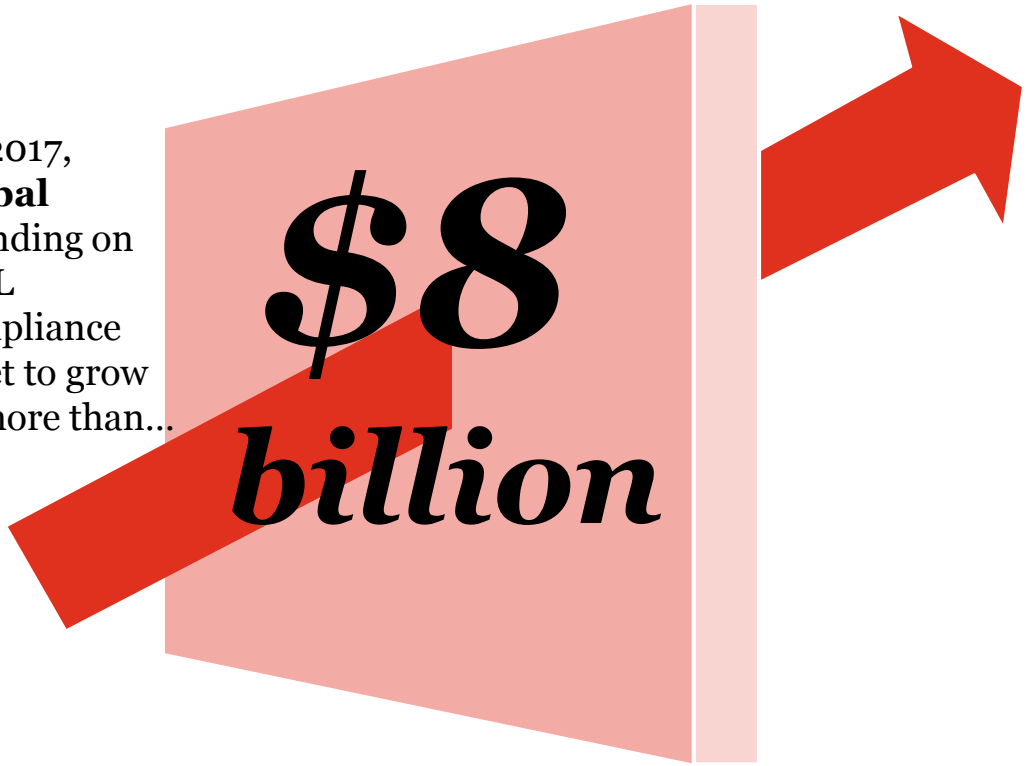
# *Money laundering destroys value*
## Global results of the survey



# *Rising costs as regulatory focus on money laundering increases*

*With the rising visibility of terrorist attacks, money laundering and terrorist financing are escalating in priority for governments across the globe*

By 2017, **global** spending on AML compliance is set to grow to more than...




## But it's not just financial services institutions

Any organisation that facilitates financial transactions – including **non-bank money service businesses such as digital/mobile payment services, life insurers and retailers** – is also coming within the scope of anti-money laundering (AML) legislation worldwide.

***Alarmingly, but not surprisingly, many of these new participants are not yet up to speed on the requirements they must meet or on the compliance programmes they will need.***

# *What does this mean for your organisation?*

***With the globalisation of AML/CFT standards, it's important to remember that you may be judged by the highest international compliance standards.***

**Here are 3 *action* points to consider:**

## 1. Keep your finger on the regulatory pulse

Look beyond mechanical compliance with today's laws. Instead, look ahead and examine how to properly structure to comply with upcoming legislative trends. Focus on having a viable function within the organisation that keeps track of pending regulations in this area.

## 2. Lead the pack; don't follow

Being in the middle of the pack exposes you to the risk of falling behind the regulatory curve. Focus on being strategically nimble and innovative to help you stay on top of the regulatory changes.

## 3. Learn from others' mistakes

Few organisations are known to actively investigate the root cause of significant issues as identified by regulators. Remediation often serves as a quick solution to address regulatory findings.

# *Your customers, your people, your risks…*

## Know your customer (KYC)

Transparency into your customer base goes beyond merely identifying and verifying the information they provide. It must be a dynamic act, and it is essential to keep monitoring for red flags and suspicious activity on a regular basis. Special attention should be paid to clients' business relationships and transactions – especially when they conduct business with persons residing in countries with weak or insufficient AML regulations.

## Your people, your processes

Global results show that hiring experienced staff is the most significant challenge faced in the AML arena in relation to the pace of regulatory change.

## Risk assessments are critical

Over the last decade, improved money laundering control measures in the formal financial systems have forced criminals to seek new ways to "move" the proceeds of their crimes. That's why regular risk assessments are crucial, enabling your organisation to identify and address the money laundering and terrorist financing risks you face – wherever and with whomever you do business.

# *Key Contacts:*


***Forensic Services, Anti-Money Laundering, Ethics & Compliance***

George Lambrou
Partner, Consulting
t: +357 22 555 728
e: george.lambrou@cy.pwc.com

Demetra Ellina
Director, Consulting
t: +357 22 555 732
e: demetra.ellina@cy.pwc.com

Nicholas Roussos
Senior Manager, Consulting
t: +357 22 555 055
e: nicholas.roussos@cy.pwc.com

***Cyber Security***

Tassos Procopiou
Partner, Consulting
t: +357 22 555 750
e: tassos.procopiou@cy.pwc.com

Efthyvoulos Efthyvoulou
Senior Manager, Consulting
t: +357 22 555 460
e: efthyvoulos.efthyvoulou@cy.pwc.com