The Impact of Financial Crime on Global Economies

EastNets
en.abling confidentiality

en.abling
GROWTH
IT'S OUR CHOICE
14TH ANNUAL CONFERENCE

London • New York • Paris • Brussels • Luxembourg • Cairo • Beirut • Amman • Dubai • Bahrain • Karachi • Hong Kong • Johannesburg

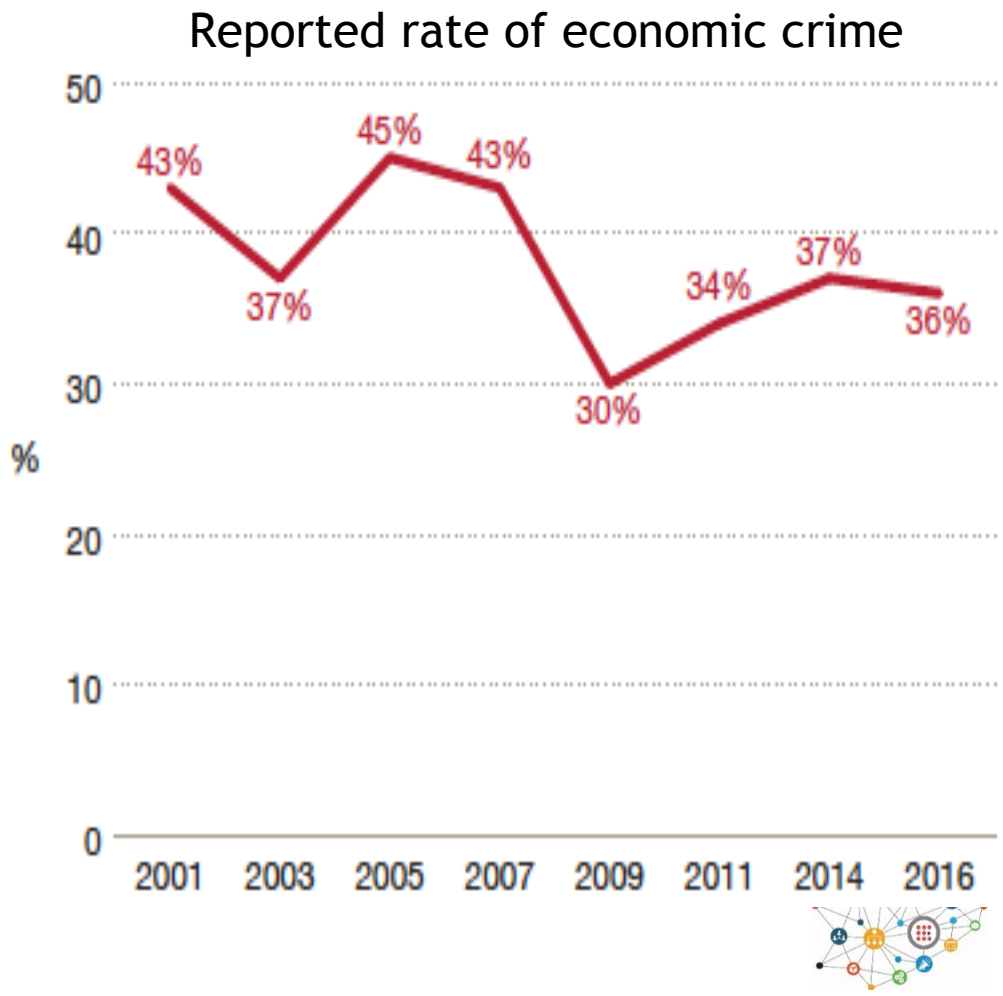
Agenda

- ✓ **Economic crime & Impact on Economic Growth**
- ✓ **Rise of the Digital Economy & Growing Risks of Cybercrime**
- ✓ **A Compliance & FinTech/ RegTech Revolution?**
- ✓ **Financial Crime Outlook**
- ✓ **Key takeaways**

What Is Economic Crime?

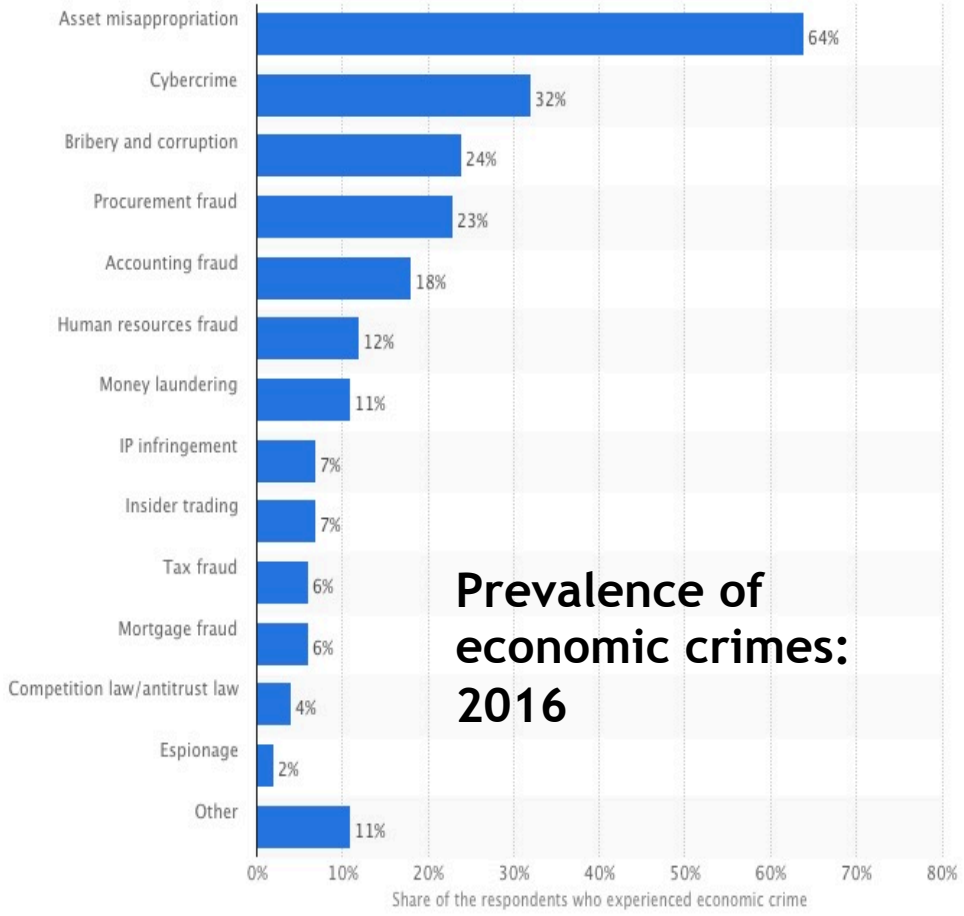
- No widely accepted single definition.
- Economic crimes refer to non-violent & illegal acts committed by an individual or a group of individuals to obtain an economic, financial or professional advantage
- Economic crimes are likely widely under-reported: 1 in 10 economic crimes are discovered by accident!

Economic crime evolving, while preventative measures lagging

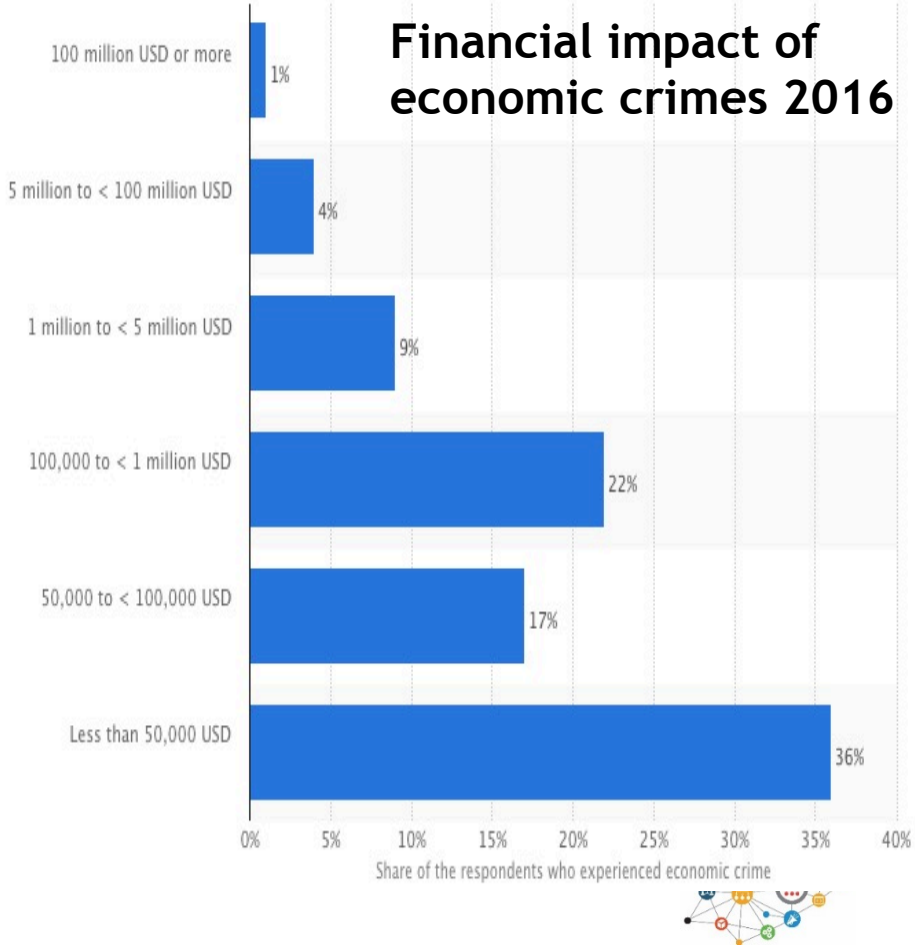


Economic Crimes & Financial Impact

- Asset misappropriation, cybercrime, bribery and corruption top crime list
- 32% of the companies experiencing economic crime were victims of **cybercrime**
- 15% of economic crimes are $1mn or more



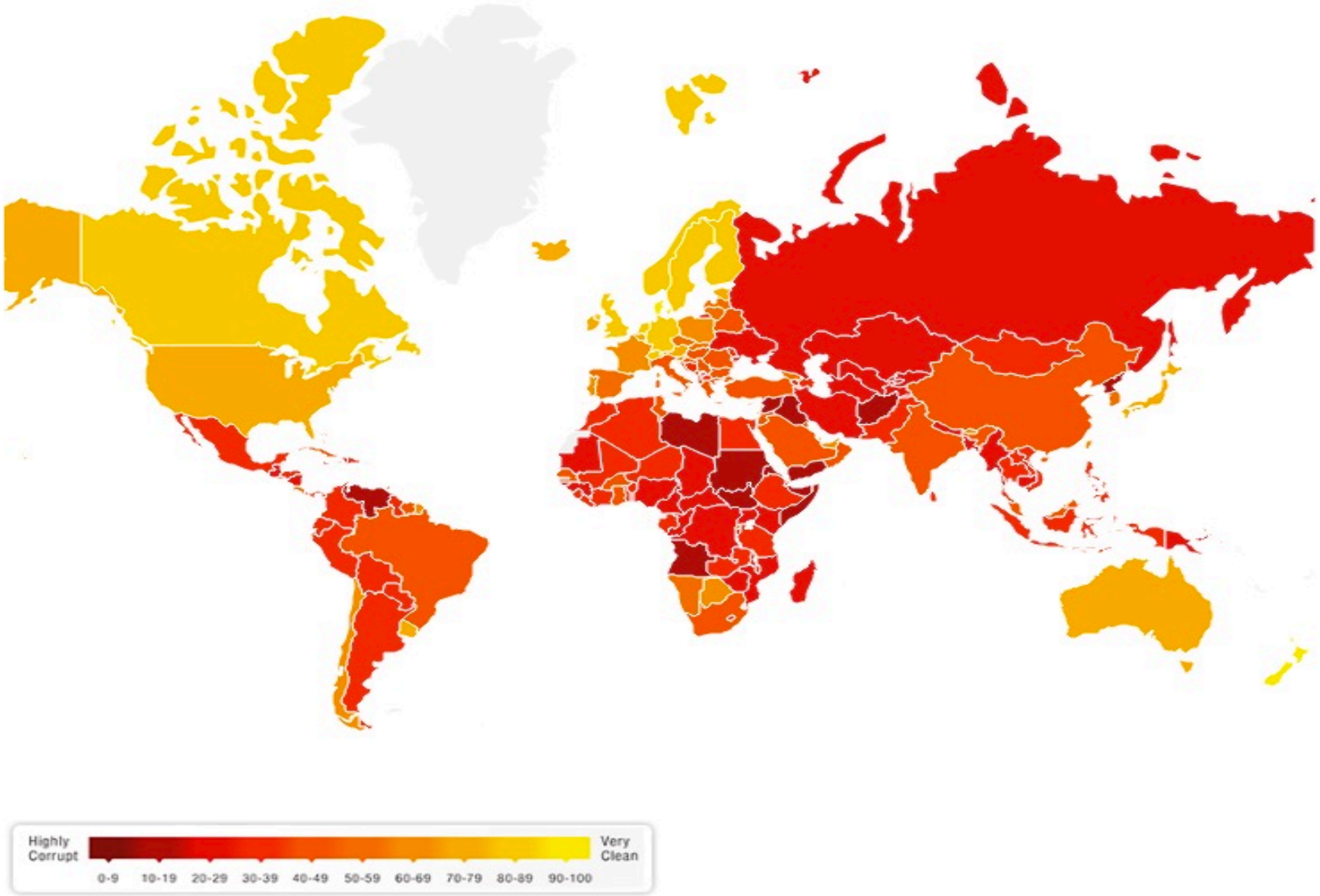
Prevalence of economic crimes: 2016



Financial impact of economic crimes 2016

Source: Global Economic Crime Survey 2016, PwC

Corruption Perception Index 2016: 90% of Arab countries score below 50. Associated with inequality and populism



Source: Transparency International

Economic Consequences of Bribery & Corruption

- Estimates show that the cost of corruption equals more than 5% of global GDP **$ 2.6 trillion** (WEF) with over **$ 1 trillion** paid in bribes each year (World Bank)
- Corruption **increases the cost of doing business by up to 10%** on average (WEF)
- Corruption distorts market mechanisms like fair competition , increases transaction costs and uncertainty and deters domestic and foreign investments, thus stifling growth, innovation and future business opportunities. **Investment in corrupt countries is 5% less** than in countries that are relatively corruption-free (IMF)
- Corruption leads to waste or the inefficient use of public resources
- Corruption excludes poor people from public services and perpetuates poverty and is associated with greater inequality
- Corruption corrodes public trust, undermines the rule of law and ultimately delegitimises the state, leading to populism

Example 1: Costs from Market Manipulations

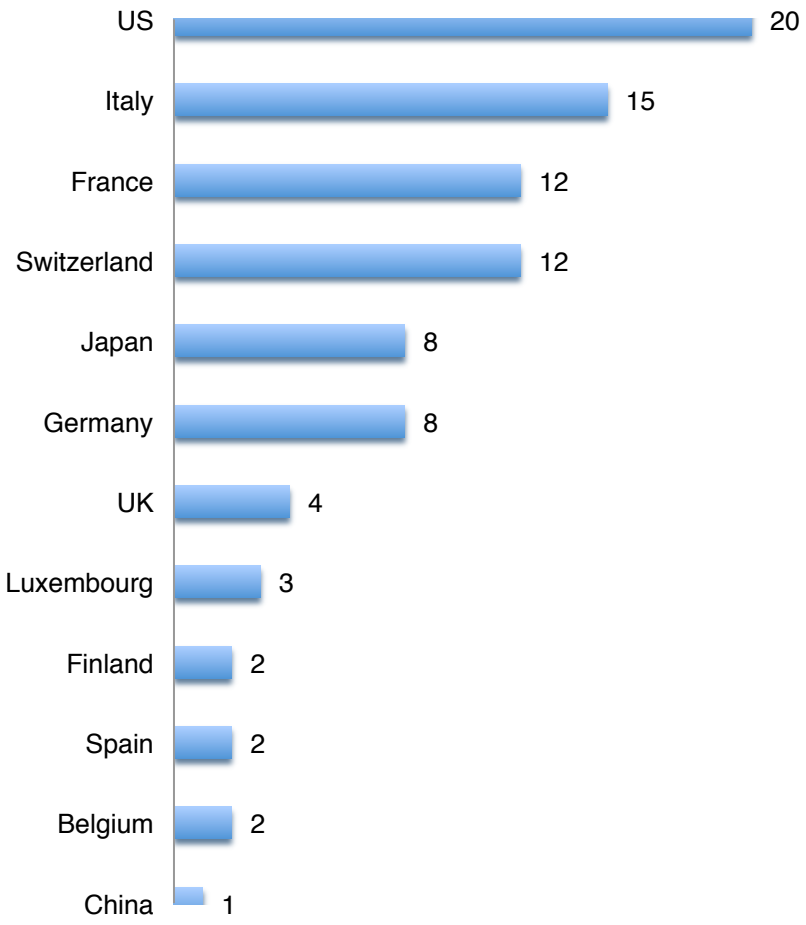
Market Manipulations	
	Churning – when a trader places both buy and sell orders at the same price. This increased activity is intended to attract other investors and increase the price.
	Painting the Tape – when a group of traders create activity or rumors to drive up the price of a stock (also referred to as “Runs” or “Ramping”).
	Wash trading – selling and re-purchasing the same security or substantially the same security to generate activity and increase the price.
	Bear raiding – attempting to push down the price of a stock by heavy selling or short selling.
	Cornering (the market) – purchasing enough of a particular stock, commodity, or other asset to gain control of the supply and be able to set the price for it.
	Insider Trading – when insiders with important confidential information about a company take advantage of that knowledge to make a profit or avoid losses by buying or selling stocks.

- The total banks have paid in fines and settlements since 2008 now exceeds $321bn (BCG)
- In 2016 alone, banks paid $42bn in fines, up 68% yoy
- In 2015, 6 global banks were fined more than $5.6bn to settle allegations that they rigged foreign exchange markets

Example 2: Global trade in fake goods worth nearly half a trillion dollars a year - OECD

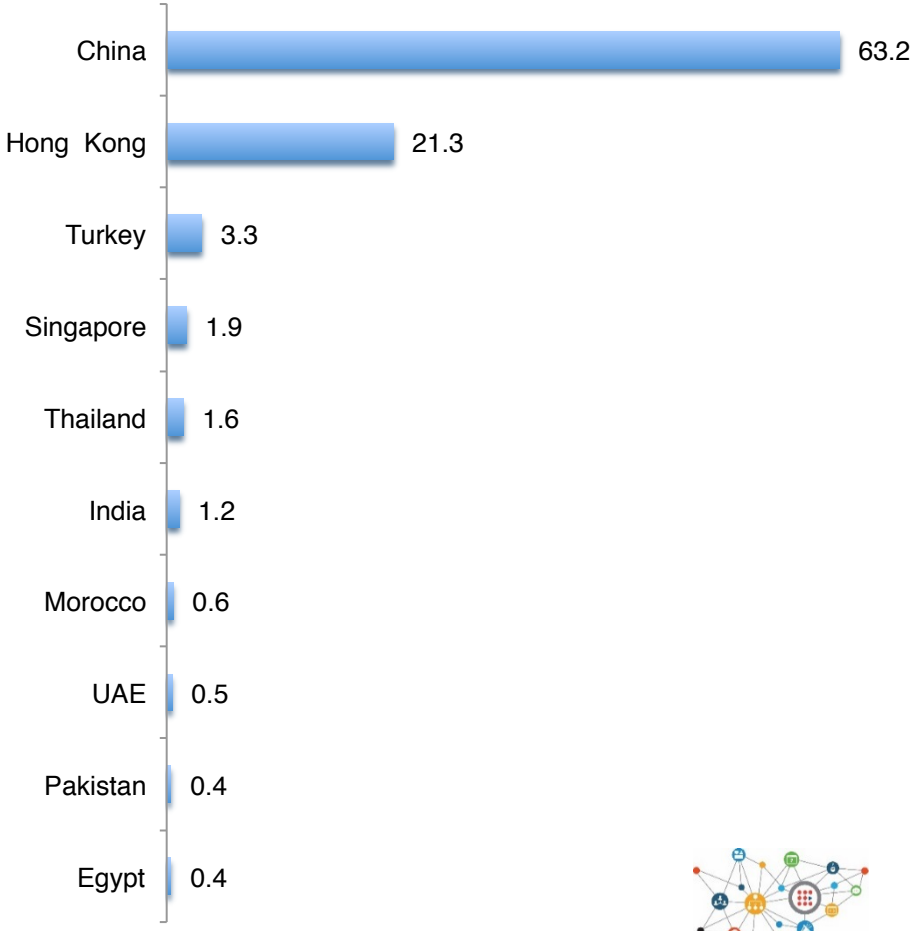
Countries hit hardest by trade in fake goods

Top countries whose IP rights are infringed, % total value of seizures (2013)



Where most fake goods originate

Top provenance economies of fakes, as % of total seizures (2013)

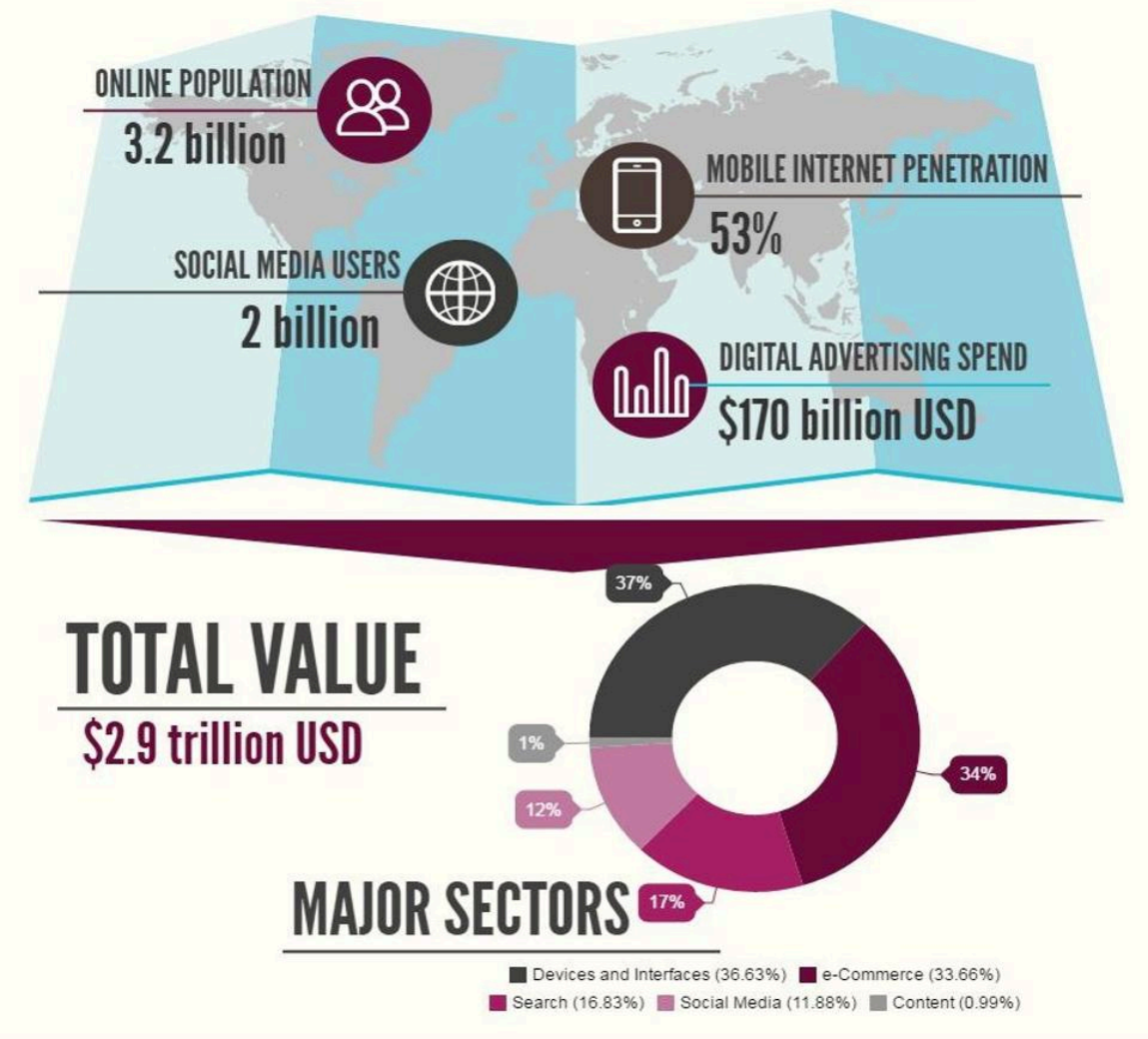


Source: Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, OECD

Agenda

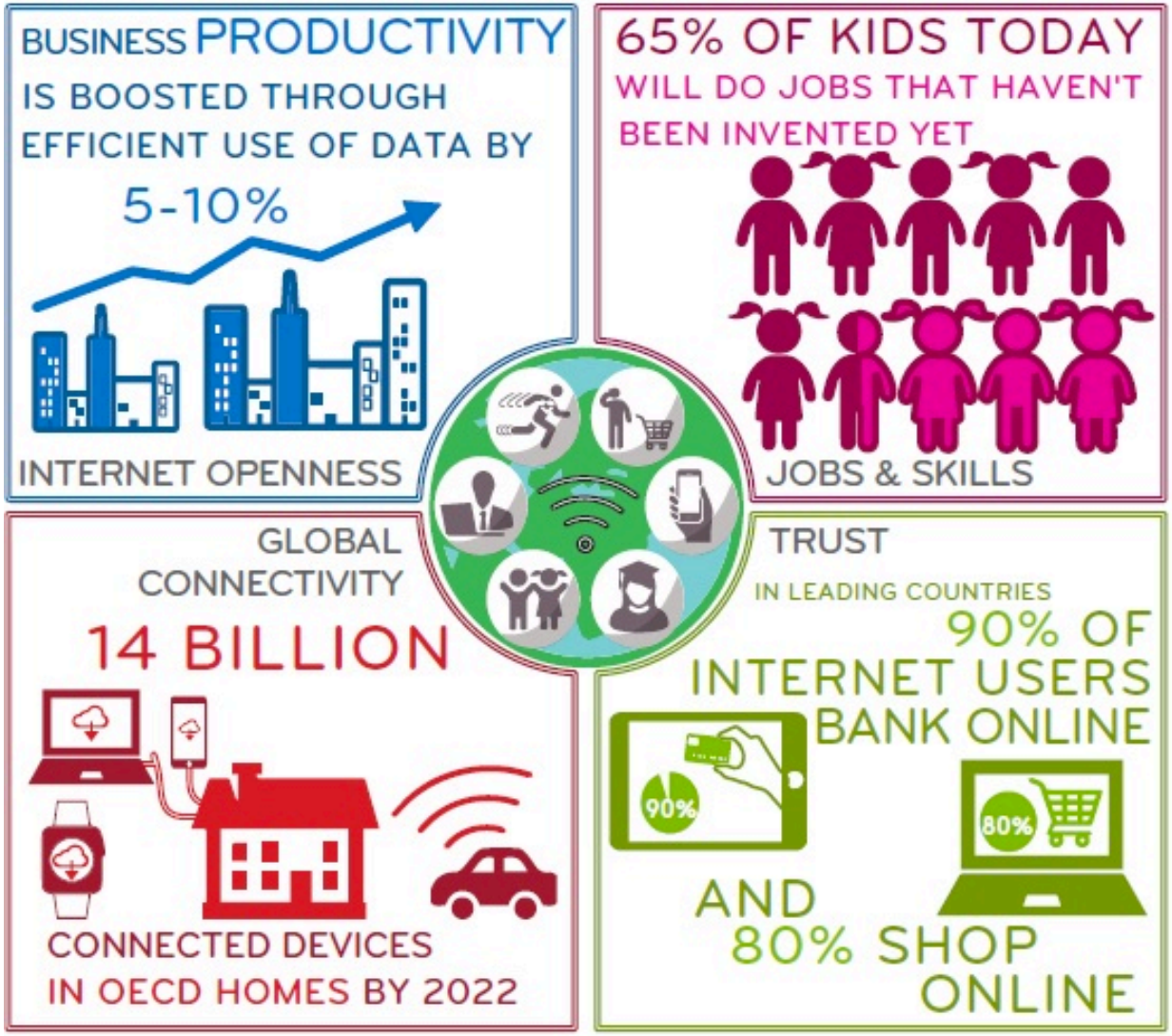
- ✓ Economic crime & Impact on Economic Growth
- ✓ **Rise of the Digital Economy & Growing Risks of Cybercrime**
- ✓ A Compliance & FinTech/ RegTech Revolution?
- ✓ Financial Crime Outlook
- ✓ Key takeaways

The exploding, ubiquitous Digital Economy



- Half the world's population is online
- A third are on a social network
- 53% are mobile
- Span all ages, races, geographies & cultures
- A young, dynamic, $3trn++ ecosystem based on technological infrastructure, increasingly interactive devices and interfaces, vast audience networks, a whole new medium for advertising and an unlimited supply of content

Policy Challenges of Tomorrow's Digital Economy



Introduction of new technologies & 'internet of everything' paves the way for growing cyber risks & crime

The Changing Faces of Crime: From the Mafia to the Hacker to a Group of Hackers

EastNets
en.abling confidentiality

THEN...

NOW...

MORE RECENTLY...

The New Face of Organized Crime

Hackers are no longer lone wolves. They're now banding together to run fewer—yet much larger—attacks, similar to the traditional crime rings of the 20th century.

80%

of cyber-attacks are driven by **organized crime rings**, in which data, tools, and expertise are widely shared.[1]

Economic Effects Of Cybercrime

Cybercrime damages trade, competitiveness, innovation, and global economic growth.

- Cost of cybercrime will continue to increase as more government and business functions move online and as more governments, companies and individuals around the world connect to the Internet.
- Losses from the theft of intellectual property will also increase as acquirers improve their ability to make use of it to manufacture competing goods.
- Cybercrime is a threat to the fast growing class of digital assets and their integrity
- Cybercrime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors.
- Governments need to begin serious, systematic effort to collect and publish data on cybercrime to help countries and companies make better choices about risk and policy

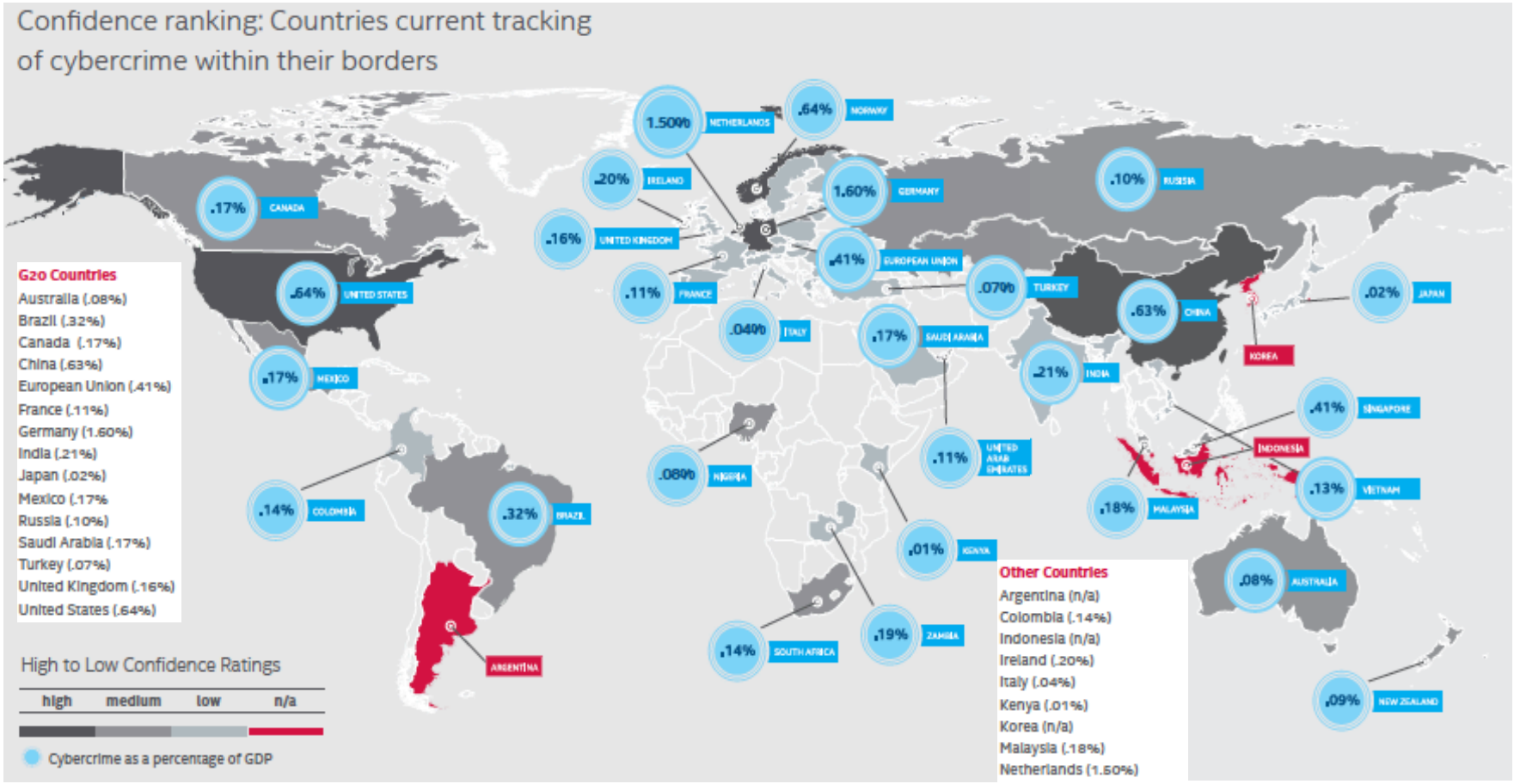
Rising Economic Costs of Cybercrime

- **Cyber crime costs the global economy about $475bn every year**; ranging between a conservative estimate of $375bn in losses to a maximum of as much as $575bn: CISS-McAfee research (2014)
- **World's biggest economies bore the brunt** of the losses: toll on US, China, Japan and Germany at $200bn
- It is estimated that the **global cost of cybercrime will reach $2 trillion by 2019, a threefold increase** vis-à-vis ~$500bn
- Just the tip of the iceberg: significant portion of cybercrime goes undetected/unreported (WEF, "The Global Risks Report 2016".
- Cybercrime has serious **implications for employment**, in the developed economies: translates into ~200k & 150k jobs lost in US & EU respectively
- Losses connected to **personal information**, such as stolen credit card data, was put at up to $150bn
- **Cybercrime is equal to between 15-20% of the value created by the Internet**: significant tax on the potential for growth & job creation

Source: Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, CISS Jun 2014, McAfee

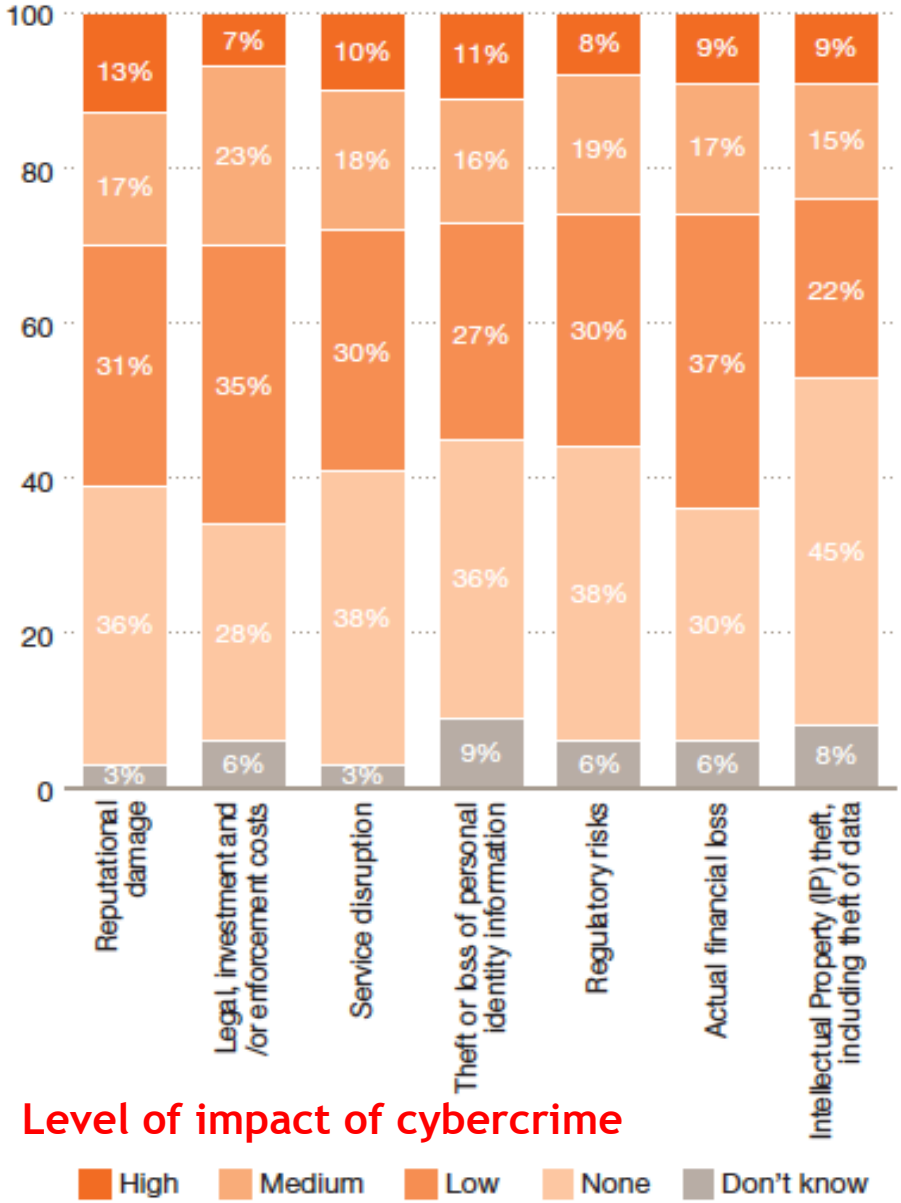
Tracking Cybercrime & Cybercrime as % of GDP: governments failing to track reduces risk to cyber-criminals

EastNets
en.abling confidentiality



Source: Net Losses: Estimating the Global Cost of Cybercrime
Economic impact of cybercrime II, CISS Jun 2014, McAfee

Cybercrime is on the Rise…



Nation-states

threats include espionage and cyber warfare - victims include government agencies, infrastructure, energy and IP-rich organisations

Insiders

not only your employees but also trusted third parties with access to sensitive data who are not directly under your control

Terrorists

still a relatively nascent threat - threats include disruption and cyber warfare; victims include government agencies, infrastructure and energy

THREAT VECTORS

Organised crime syndicates

threats include theft of financial or personally identifiable information (sometimes with the collusion of insiders) - victims include financial institutions, retailers, medical and hospitality companies

Hacktivists

threats include service disruptions or reputational damage; victims include high-profile organisations and governments - victims can include any kind of organisation

Source: Global Economic Crime Survey 2016, PwC

the answer company™ THOMSON REUTERS®

Deloitte.

FINANCIAL CRIME SURVEY 2017

JANUARY 2017

61% ARE CONCERNED ABOUT **MANAGING COSTS** ASSOCIATED WITH **FINANCIAL CRIME PROGRAMS**

75% OF RESPONDENTS ARE CONFIDENT THAT THEIR **TECHNOLOGICAL SOLUTIONS** ARE OPERATING AS REQUIRED

BUT **45%** DESIRE BETTER **ANALYTICAL AND DATA MANAGEMENT FUNCTIONALITY** FROM THEIR TECHNOLOGY

65% REPORT **INCREASING COMPLIANCE BUDGETS** OVER THE PAST **2 YEARS**

63% OF RESPONDENTS EXPECT THIS TREND **TO CONTINUE**

2016 2017 2018

43% OF RESPONDENTS **LACK CONFIDENCE IN THEIR FINANCIAL CRIME PREVENTION PROGRAM**

80% REASSESS THEIR **FINANCIAL CRIME -RELATED RISKS AT LEAST ONCE A YEAR**

86% OF RESPONDENTS ARE **CONCERNED ABOUT CYBER CRIME** BUT ONLY **47% HAVE A CYBER CRIME POLICY**

86% 47%

INCREASING COMPLIANCE ACTIVITY

MORE TRAINING

INCREASED PERSONNEL HOURS

HIGHER INVESTMENT IN TECHNOLOGY

INCREASED STAFF RESOURCES

MORE TIME MONITORING

INCREASED COMMUNICATION

NEW PROCESSES

COMPLIANCE SPEND WHERE IS THE MONEY GOING?

TECHNOLOGY

TRAINING*

PROCESS**

RECRUITMENT

REGULATORY INTELLIGENCE

SKILLS

OUTSOURCING COMPLIANCE

*compliance department & wider business
**internal business change & reorganization

*Source: Financial Crime in the **Middle East and North Africa** 2017*

Top 5 Compliance Trends Around the Globe in 2016

- Creating a culture of compliance
- Increased investment in compliance operations
- Keeping pace with a changing regulatory landscape
- Encouraging whistleblower activity
- Monitoring third-party risk

of businesses surveyed viewed promoting a corporate culture of integrity to be the ultimate goal of their compliance and ethics programs

Increased Investment in Compliance Operations

Last year, 71% of firms expected the cost of senior compliance professionals to increase due to the demand for skilled/knowledgeable staff

This trend continues in 2016 with a high proportion of boards predicting a "significant increase" in compliance spending:

75% of compliance leaders expect management will require more/much more attention

51,000+

REGULATORY AND COMPLIANCE UPDATES IN 2015

More than 1/3 of organizations surveyed **spend at least an entire day per week** tracking and analyzing regulatory change

Regulatory focus:

Personal Liability

93% of practitioners voting at the 2015 Thomson Reuters New York Customer Summit expected the personal liability of compliance professionals to increase in 2016

64% of respondents to the Thomson Reuters personal liability survey expected that individual accountability would be replicated around the world

Behavioral-Based Regulations

Conduct-related infractions are projected to exceed **$20B** globally

Exposure to risk:

6,000+ names of companies/ individuals on OFAC's Specially Designated Nationals and Blocked Persons List

Fines of up to US $20M and imprisonment up to 30 years for OFAC violations

US Securities and Exchange Commission collected $114.8 million in 2015 Foreign Corrupt Practices Act enforcement actions

Encouraging Whistleblower Activity

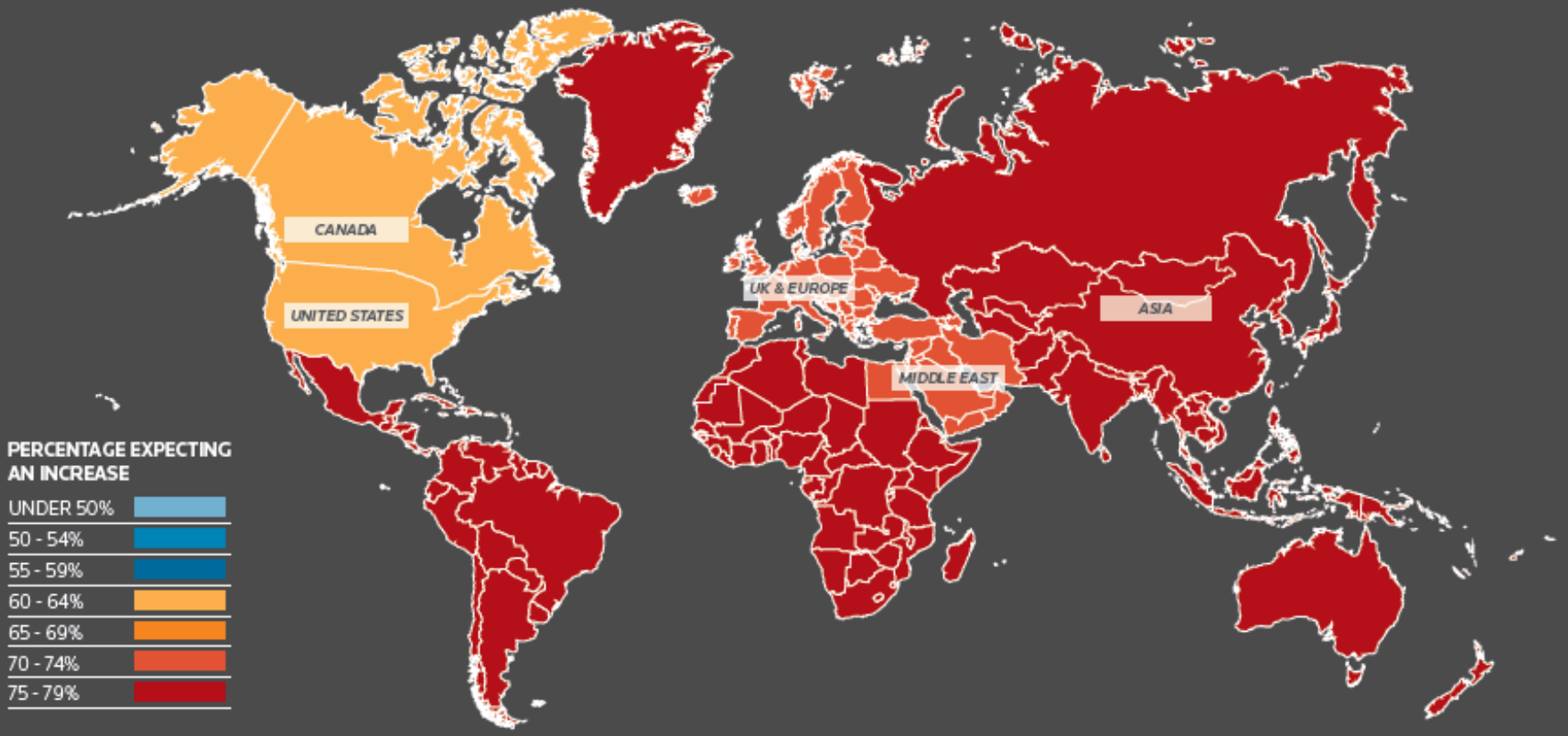
US SEC received 4,000 whistleblower tips and paid $37M in whistleblower rewards in 2015

SOURCES:

1 Thomson Reuters Cost of Compliance Survey 2015
2 Thomson Reuters Rising Personal Liability – Perception and Reality: How Best to Manage Personal Regulatory Risk
3 Thomson Reuters White Paper – What's Compliance Worth?
4 Thomson Reuters White Paper – How to Manage Conflicts of Interest: A Question of Culture
5 Thomson Reuters Regulatory Intelligence
6 KPMG Anti-Bribery and Corruption Survey

Sources: Thomson Reuters Risk and KPMG Anti-Bribery and Corruption Survey

REGIONS EXPECTING THAT COSTS OF SENIOR COMPLIANCE STAFF WILL **INCREASE SLIGHTLY OR SIGNIFICANTLY** IN THE COMING YEAR



Over the next 12 months, I expect the cost of senior compliance staff to be...	UK & EUROPE	US & CANADA	ASIA	MIDDLE EAST	REST OF THE WORLD
More than today	**70%**	**60%**	**77%**	**72%**	**79%**
The same as today	26%	34%	20%	28%	17%
Less than today	4%	6%	3%	0%	4%

Spending more on compliance doesn't translate immediately into lower crime: Governance & Integrity matter

Source: The Cost of Compliance 2016, Thomson Reuters

Agenda

- ✓ Economic crime & Impact on Economic Growth
- ✓ Rise of the Digital Economy & Growing Risks of Cybercrime
- ✓ **A Compliance & FinTech/ RegTech Revolution?**
- ✓ Financial Crime Outlook
- ✓ Key takeaways

The Future of Compliance: FinTech/ RegTech

- Risk & compliance involvement in assessing the implications of FinTech innovation: 42% respondents reported some involvement but not enough; 21% fully engaged & consulted.
- **Skill sets have grown**: 56% have widened the skill set w/n risk & compliance functions to accommodate developments in FinTech and RegTech innovation and associated digital disruption; 15% reported investing specifically in specialist skills.
- **RegTech has begun to shape compliance**. More than half (52%) considered that RegTech solutions were affecting how they managed compliance in their firms with almost a fifth (17%) reporting they have already implemented one or more RegTech solutions.
- **RegTech has the potential to affect a wide range of compliance activities.** The top three areas reported as likely to be affected by RegTech: compliance monitoring (47%), regulatory reporting (40%) and capturing regulatory change (35%).

Source: FinTech, RegTech and the role of compliance, Thomson Reuters Dec 2016

FinTech: Implications for Supervisors & Regulators

1. Regulators & Supervisors need greater engagement and dialogue with the private sector and innovators.
2. Regulators & Supervisors need to build capacity to do their jobs.
3. Banking & Financial regulators will need to cooperate more with other authorities at the national level as the borders between technology, finance, payments and digital activities coalesce.
4. Technology and finance span national borders. Cybercrime does not respect borders. Cooperation & exchange of information at the international level is essential.

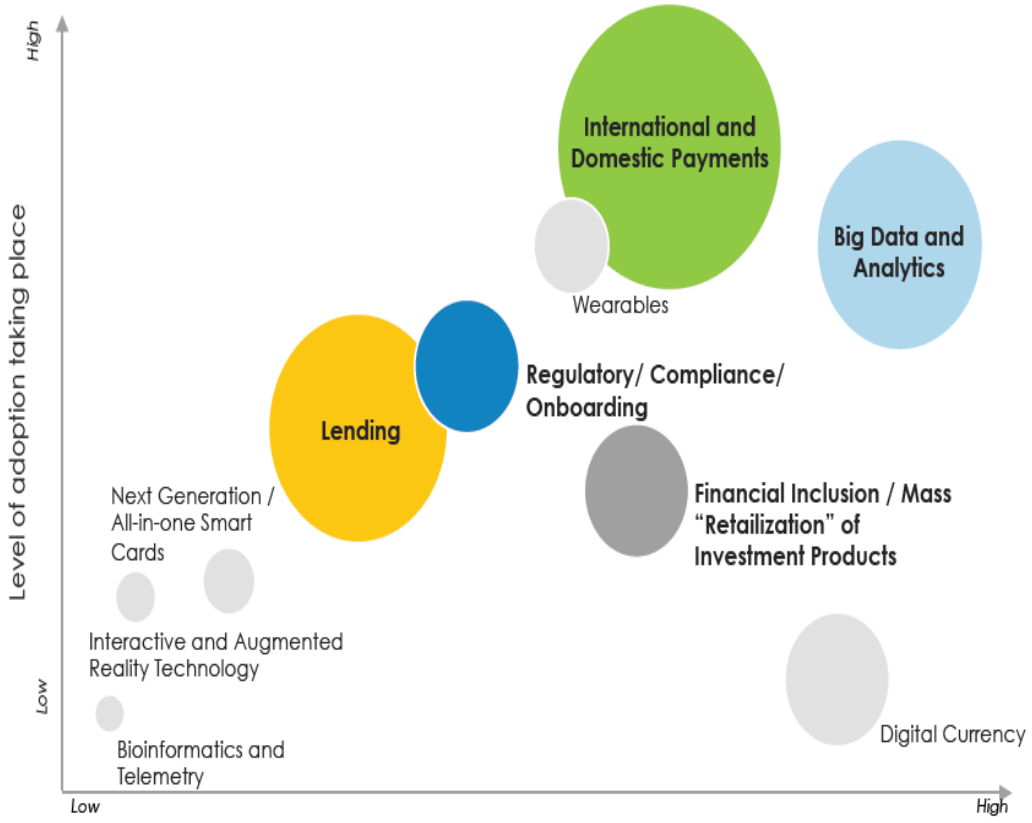
RegTech will help firms to automate the more mundane compliance tasks and reduce operational risks associated with meeting compliance and reporting obligations

EastNets
en.abling confidentiality

Key characteristics of RegTech:

1. **Agility**: cluttered and intertwined data sets can be de-coupled and organised through ETL (Extract, Transfer Load) technologies
2. **Speed**: Reports can be configured and generated quickly
3. **Integration**: short timeframes to get solutions up and running
4. **Analytics**: RegTech uses analytic tools to intelligently mine existing "big data" data sets; e.g. using the same data for multiple purposes

FinTech companies have the potential to address defined business problems & fill capability gaps



"We are drowning in information, while starving for wisdom"
- Edward Wilson, biologist

How can Big Data/ Machine learning/ Data Science support AML?

Big Data presents an opportunity to improve transaction monitoring & KYC processes + help AML/CFT

Firms need to invest in real time, high quality sources & combinations of data, & advanced analytics to help reveal the relationships between individuals, transactions, & events in real time.

Machine Learning can be used to:

- Learn transaction behavior for similar customers. Pinpoint customers with similar transactions behavior. Identify outlier transactions and outlier customers
- Discover transaction activity of customers with similar traits (business type, geographic location, age, etc.)
- Learn money laundering typologies and identify typology specific risks
- Dynamically learn correlations between alerts which produced verified suspicious activity reports
- Continuously analyze false-positive alerts and learn common predictors

Agenda

- ✓ Economic crime & Impact on Economic Growth
- ✓ Rise of the Digital Economy & Growing Risks of Cybercrime
- ✓ A Compliance & FinTech/ RegTech Revolution?
- ✓ **Financial Crime Outlook**
- ✓ Key takeaways

Financial Crime Topics for 2017

- **Slowdown in new regulation**: focus on effective compliance with existing regulations
- **Convergence of financial and cyber crime** => a coordinated response; threat assessments for new digital products or digitized activities
- **Big Data**: use of data to help prevent & detect financial crime; increased use of AI & machine learning
- **Biometrics & Blockchain**: use of biometrics + digital identity => potential to transform customer onboarding
- **Outside the banking sector**: focus by regulators on the effectiveness of anti-financial crime controls in insurance, asset management & private wealth management sectors
- **Technology trends**: acceleration in development and use of new technology solutions for transaction monitoring & data analytics

Source: Financial Crime Unit, PwC, 2017

New Developments to be prepared for…

Global Regulatory Outreach & International Cooperation: interconnected networks => no "borders"

Emerging Regulations: Economic Sanctions, "5th" EU Directive AML

Threats Re-loaded: e.g. financing of terrorism

New Technologies: Blockchain, Bitcoin, KYC utilities

Regulation of digital currency exchangers and wallet providers

Common Reporting Standards, Tax fraud

Expectations of authorities: Forensic readiness, e-discovery, transaction monitoring, risk assessment

Source: Financial Crime Unit, PwC, 2017

Agenda

- ✓ Economic crime & Impact on Economic Growth
- ✓ Rise of the Digital Economy & Growing Risks of Cybercrime
- ✓ A Compliance & FinTech/ RegTech Revolution?
- ✓ Financial Crime Outlook
- ✓ **Key takeaways**

Key Takeaways I

- Economic crime results in lower trade, investment and growth and diversion of private sector resources to security & protection of assets and transactions
- Economic crime is big and growing. Financial crime is the nexus.
- Cyber crime and financial crime will increasingly converge.
- Economic crime and criminals respond to incentives, to costs & benefits
- Growth of digital economies have widened the scope and lowered the cost of cybercrime both with countries and cross-border → growing risks
- Growing economic weight of more vulnerable emerging economies increases scope and risk of cybercrime
- Arab countries increasingly vulnerable to cybercrime as they enter digital era
- Financial cybercrime will tend to grow faster as demand for financial services grows faster than income

Key Takeaways II

- Financial/cyber crime exposes banks & financial institutions to large potential losses including loss of confidence and trust
- Growing bank disintermediation and rise of FinTech increases risk and scope of cybercrime
- Wider use of digital technologies has a dark side in the increasing pervasiveness and scale of cyber-attacks, posing privacy, security and integrity threats.
- But Fintech & Regtech have potential to revolutionise regulation & compliance and effectively combat cybercrime
- Cybercrime requires international cooperation between sovereigns, specialised agencies, regulators, IT, network operators & tech companies

Selected Readings

- *BIS (2016): "Financial inclusion and the fintech revolution: implications for supervision and oversight", Oct*
- *Booz Allen Hamilton (2016): "Five Quick Wins for AML Efficiency", Feb*
- *CISS/ McAfee (2014): "Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II", Jun*
- *Deloitte: "The Future of Regulatory Productivity", RegTech position paper*
- *Deloitte (2015): "RegTech is the new FinTech"*
- *OECD (2014): Issues Paper on Corruption and Economic Growth*
- *OECD (2014): The Rationale for fighting corruption*
- *PwC (2017): "Fight against Financial Crime: overview on trends and developments", Financial Crime Unit, Feb*
- *Pricewaterhouse Cooper (2016): "Global Economic Crime Survey 2016"; available at www.pwc.com/crimesurvey*
- *Thomson Reuters & Deloitte (2017): "Financial Crime in the Middle East and North Africa 2017"*
- *Thomson Reuters (2016): "FinTech, RegTech and the role of compliance", Dec*
- *Thomson Reuters (2016): "Cost of Compliance 2016"*
- *Thomson Reuters Risk & KPMG (2016): "Anti-Bribery and Corruption Survey"*
- *Transparency International (2017): Corruption Perception Index 2016*

EastNets®
en.abling confidentiality

Dr. Nasser Saidi
Email: info@nassersaidi.com
Twitter: @NSA_economics
Website: http://www.nassersaidi.com

THANK YOU