KPMG

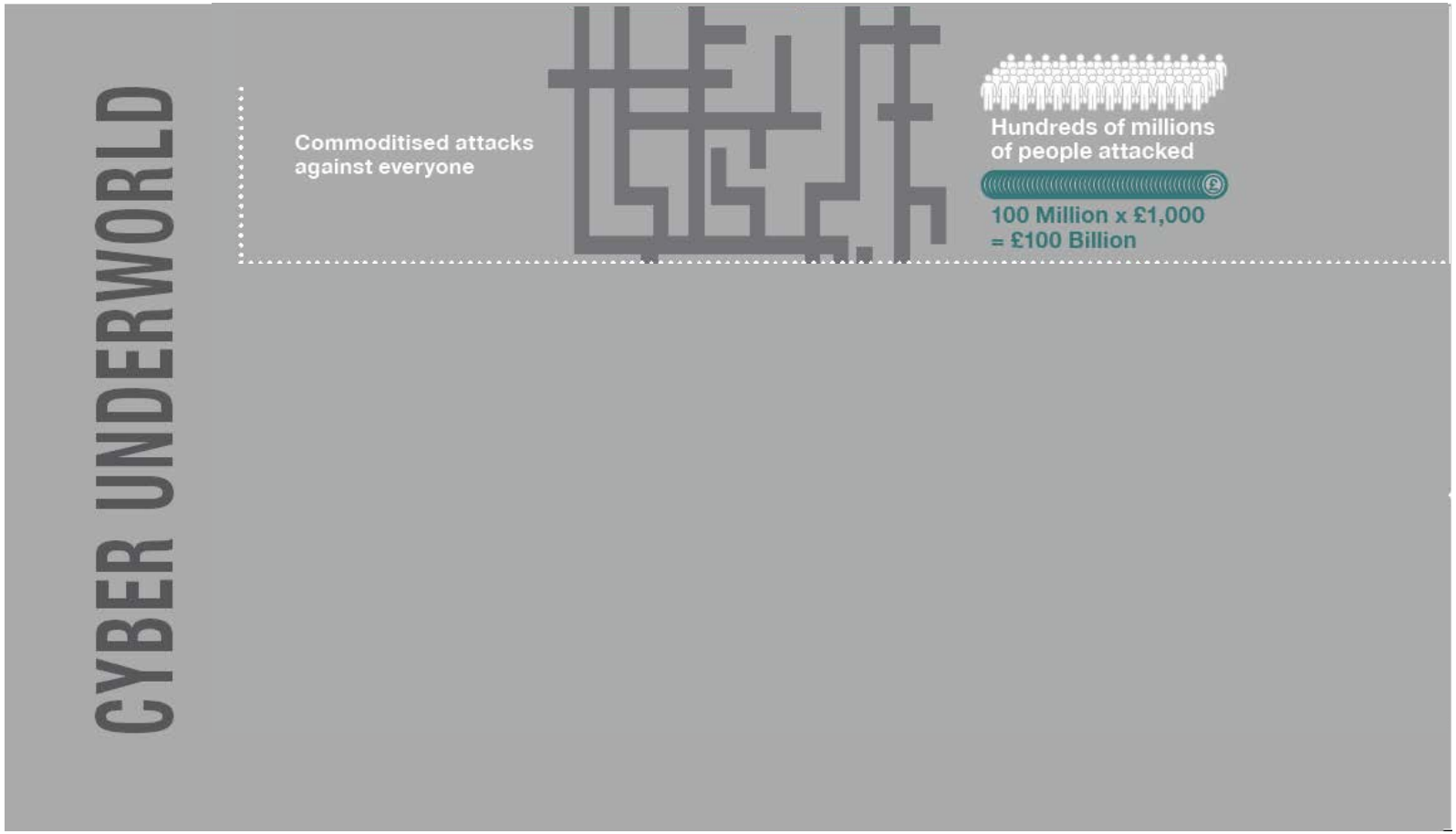
Cyber Security Challenges

16th August 2018

Talking points

- The threat landscape
- The regulatory response
- The journey towards cyber security
- The board challenges

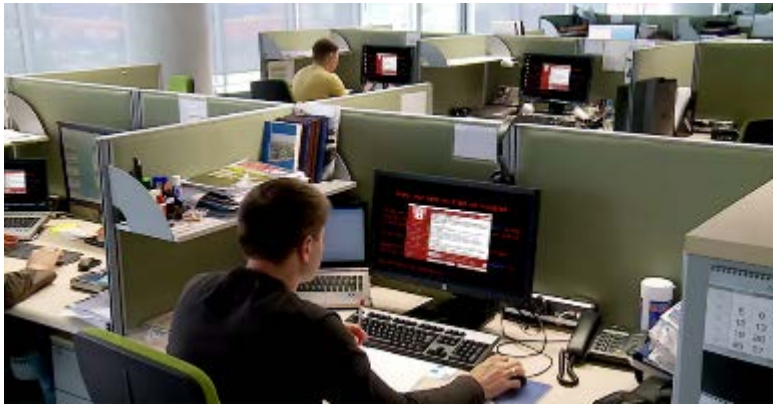
Cyber Crime Landscape



Commodity Crime

Endemic Ransomware and Crypto Mining

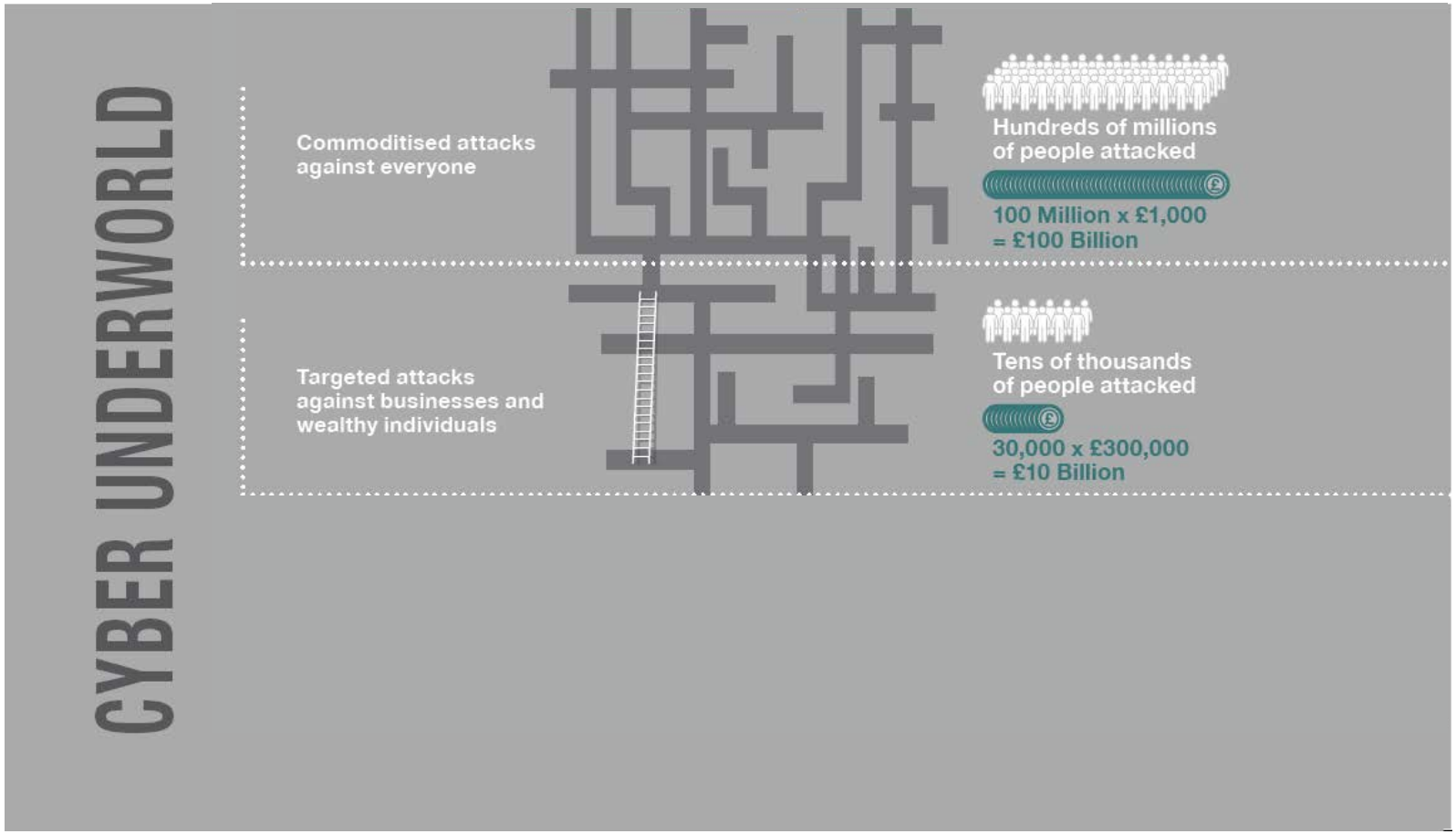
Ransomware is endemic. Rapid expansion in the range of ransomware being used as attackers move to a "Crime as a service" model. Indications that attackers are becoming more sophisticated in their extortion attempts. Mining of crypto currency using compromised computers on the rise.



Industrialisation of Cyber Crime

Large scale industrialisation of cyber crime activity exploiting cheap sources of labour. Blending technical and business skills. Operation Firstlight example of scale and sophistication of social engineering operations.

Cyber Crime Landscape



Targeted Attacks

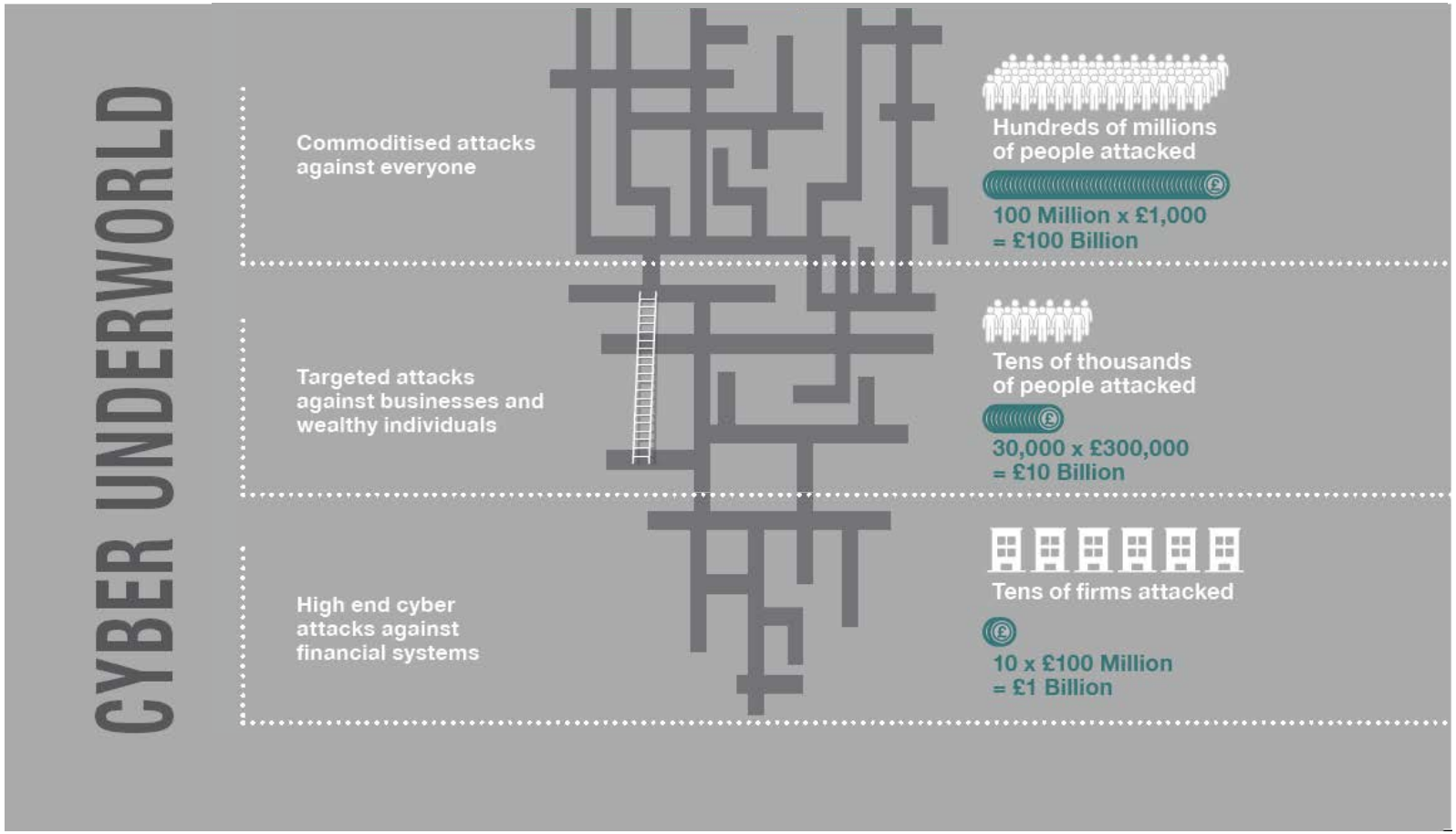
Targeting of treasury/finance/procurement

Increased targeting of corporate treasury, finance controller, and procurement functions. Part of ongoing pattern of CEO frauds and business email compromise frauds – a combination of social and technical attacks resulting in highly tailored spear phishing.

Financially Sophisticated Criminals

Growing evidence of organised crime groups becoming more financially savvy. Attacking payment systems such as SWIFT with high profile examples such as Bank of Bangladesh – but also copy cat attacks. Unlimited cash out frauds continue.

Cyber Crime Landscape



High End Attacks

A new model for cyber espionage

A shift from traditional signals intelligence through interception of communications, to the compromise of end points and telecommunication infrastructure. Long term persistent access to systems, including manipulation of lawful intercept and SS7 routing infrastructure.

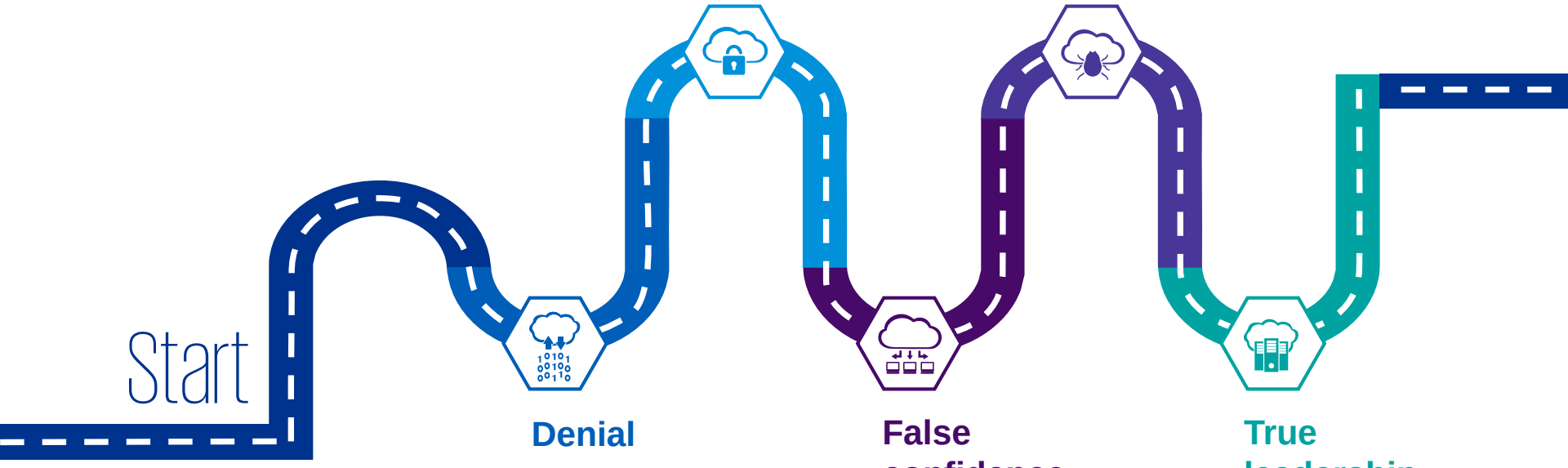
The growth of cyber warfare

30 countries worldwide believed to be developing offensive cyber attack capabilities. Initial disruptive use of cyber attack methods and tools – Ukraine has become a testbed with attacks on electrical grids and telecommunication systems.

Regulatory Landscape

- Global agenda point for regulators emerging consensus across G7
- Meeting the requirements of multiple regulators remains challenging
- Key themes:
  - Privacy (GDPR)
  - Governance/Risk Management
  - Frameworks and Independent Review
  - Third Parties/Supply Chain Security
  - Transparency/Incident Reporting
  - Threat Intelligence and Information Sharing
- Worries over systemic risk
- Growing concerns over militarisation and critical national infrastructure
- International norms of cyber security remain unclear

Journey to Cyber Security



Denial

Sometimes some lazy reporting…

And a lack of insights into the real threat

Assumes a targeted approach to crime

Ignores reality of commoditised attacks

This is all media hype anyway…

It's all teenage hackers

Nobody's interested in my firm

It hasn't happened to anyone I know

Statistics say otherwise…

But media reporting isn't exactly unbiased

A lack of transparency around cyber attacks

And just a little confirmation bias

Worry

No one every got sacked for following process

Tick boxes save hard choices

All the security firms say it's really scary

I'm getting tired of the FUD

I can buy my way out of this problem

I have policies, I have compliance, problem solved

It's impossible to stop this so why bother

Security isn't my problem… ask the IT guys

Technology or snake oil?

Lots of flashing lights

The CIO or CISO can fix it for me

And if they don't I know who to blame

False confidence

But you start to question the investment

And the world moves on

The business and its leadership set the tone

People do what they are incentivised to do…

More mystique…

And perhaps a sacrificial lamb

We're there… I'm confident

Bring it on…

Hard lessons

Did we really know how to integrate, run and support all that tech?

And what about people…

But just where does your business start and stop?

And which bits can you never outsource…

Time to slaughter the lamb

Beware the knee jerk reaction

Is adding more controls the answer?

How do you measure the opportunity cost?

True leaders

Governance is good

But commitment and ownership is better

Or are they just the future and we are the past

A new CISO role is emerging

We're in this alone

Twice a year is fine for this stuff

Digital are different

Cyber security will be around in 5 years

It's tempting to assume you are unique

But criminals (and states) don't work that way

It doesn't mean much now

It will mean even less shortly…

Hard questions to ask

How secure are we and how do we compare to our competitors?

Are we getting more or less secure?

How do we set priorities and determine risk appetite ?

Are we getting value for our cyber security spend?

How do we manage third party suppliers?

How are we organised to manage cyber risk?

And finally…

Cyber security is about harnessing digital opportunities with confidence

Not about getting in the way of doing business

It is not about technology – it is about business strategy and culture

By demanding of your cyber security team

But show you own the issue as senior leaders

KPMG

Thank you