

Revolution or evolution?

Information Security 2020

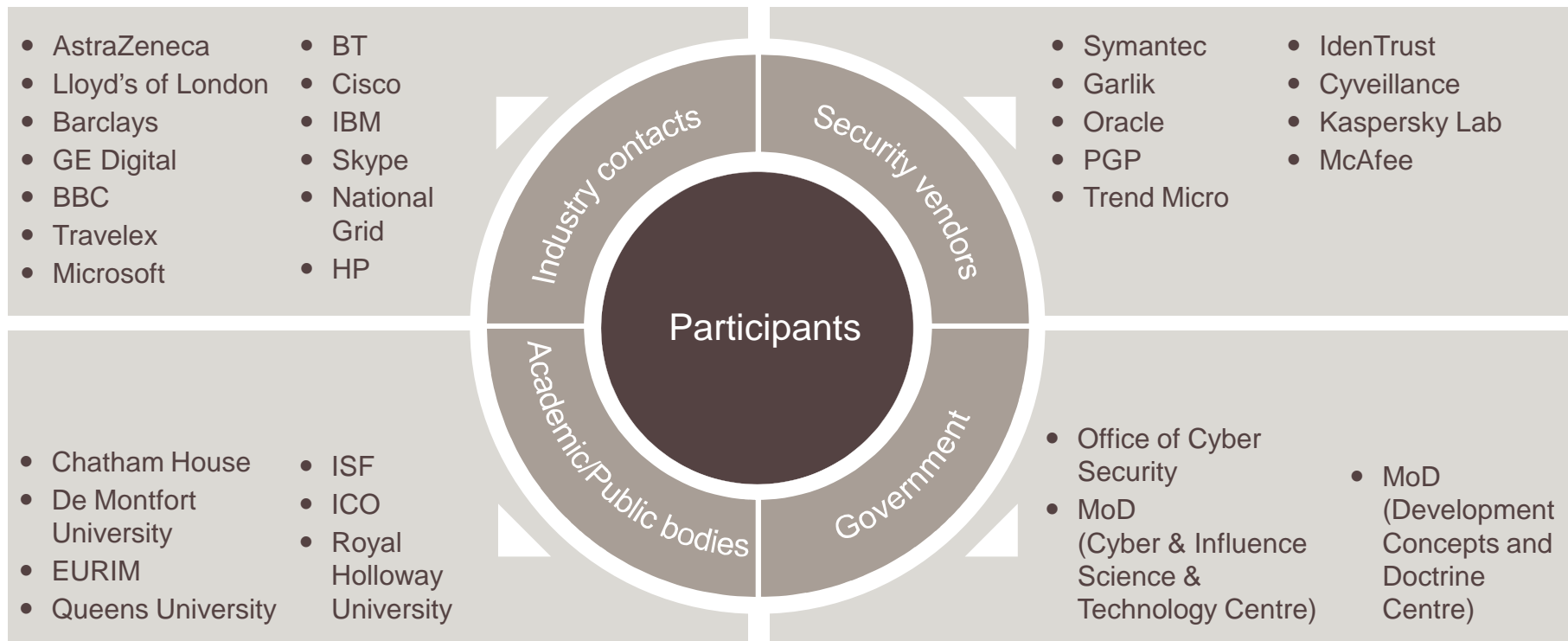
William Beer
RUSI – October 13th 2010



We drew on expert views

- We interviewed over 35 leading Information Security experts and business leaders across the private sector, academia and government
- We subsequently held a workshop with over 40 experts to explore the issues in more detail

A selection of the research participants:



Revolution or evolution?

Evolution

- The traditional view of Information Security is one of risk **mitigation**
- The **Return on Security Investment** concept is used primarily to justify expenditure on specific security initiatives or solutions

Revolution

- Organisations will increasingly recognise that a holistic approach to Information Security can provide **differentiation** and **competitive advantage**
- For organisations that do not adapt, the cost of **inaction** will increase over time

There are a broad range of emerging drivers

- Organisations are now realising that **processes and people** are overlooked components when developing approaches to Information Security.
- By 2020, there may be a **reversion to technology driven** by significant increases in the volume of data, speed of processing and communication technology, and the emergence of more complex and automated threats.

1

Infrastructure revolution

2

Data explosion

3

An always-on, always-connected world

4

Future Finance

5

Tougher Regulation and Standards

6

Multiple Internets

7

New Identity and Trust Models

1 Infrastructure revolution

Communication infrastructure is likely to evolve in a number of ways:

- Substantial increase in penetration of high speed broadband and wireless networks
- **Centralisation of computing resources and widespread adoption of cloud computing**
- Proliferation of IP (internet protocol) connected devices and growth in functionality
- **Blurring work/personal life divide and ‘Bring Your Own’ approach to enterprise IT**
- Evolution in user interfaces and emergence of potentially disruptive technologies

2 Data explosion

- Not only is the volume of electronic data at rest and in transit expected to grow rapidly, the nature of data itself will evolve.
- Over the next decade, there is likely to be:
 - **Greater sharing of sensitive data between organisations and individuals**
 - A multiplication of devices and applications generating traffic
 - A significant increase in visual data
 - More people connected globally
 - Greater automated traffic from devices
 - **A greater need for the classification of data**

“ *In the future we might see more automated attacks. If have a machine that can data mine you from social networking sites, making highly customised, realistic looking threats. There is also likely to be more targeting of high value individuals or high value groups.* ”
Cyber Security Expert

3 An always on, always connected world

Connectivity is set to increase significantly over the next decade in a number of ways:

- **Greater connectivity between people driven by social networking and other platforms**
- Increasingly seamless connectivity between devices
- Increasing information connectivity and data mining
- **Increased Critical National Infrastructure and public services connectivity**

“ Security will become the enabler. It will allow individuals living in tomorrow’s collaborative world to use any device they want for personal or business uses. Virtual business applications will run on these devices, using federated security services provided through the cloud.

Jason Creasy
Information Security Forum

”

4 Future Finance

A significant proportion of cyber crime is financially motivated and key developments in e-finance over the next decade could include:

- Rising levels of electronic and mobile commerce and banking
- **Growth in new payment models**
- Development of new banking models
- **Emergence of digital cash**

“ There is demand for anonymous electronic payments. There is no current equivalent to cash and even the new contactless payment cards leave a paper trail. ”
Cyber Security Expert

5 Tougher regulation and standards

Regulation and standards will be important drivers of Information Security over the next decade, but will need to keep pace and evolve as technology and its uses develop.

There appear to be three key themes that could impact Information Security over the next decade:

- **Increasing regulation relating to privacy**
- Globalisation and net neutrality as opposing forces to regulation and standardisation
- **Increasing standards on Information Security**

“ Privacy will be profoundly shaped by companies’ desires to share information for business intelligence and derive revenue from direct and interactive marketing, the increasing inclusion of specific security controls in privacy laws, and the changes and investment in healthcare information used and the advent of electronic health records.

Jim Koenig,
PricewaterhouseCoopers LLP (US)

”

6 Multiple internets, will one size fit all?

The internet may multiply over the next decade. There are a number of trends that could potentially lead to segmentation of the web:

- Greater censorship
- Political motivations driving new state/regional internets
- **New more secure internets**
- Evolution in user interfaces and emergence of potentially disruptive technologies
- **Closed social networks**
- Growth in paid content

“
In the future, there may be a centralised agency overseeing the internet law enforcement function. There may even be two levels of the internet – the policed bit and the anarchic bit.

Julia Harris, BBC”

7 New identity and trust models

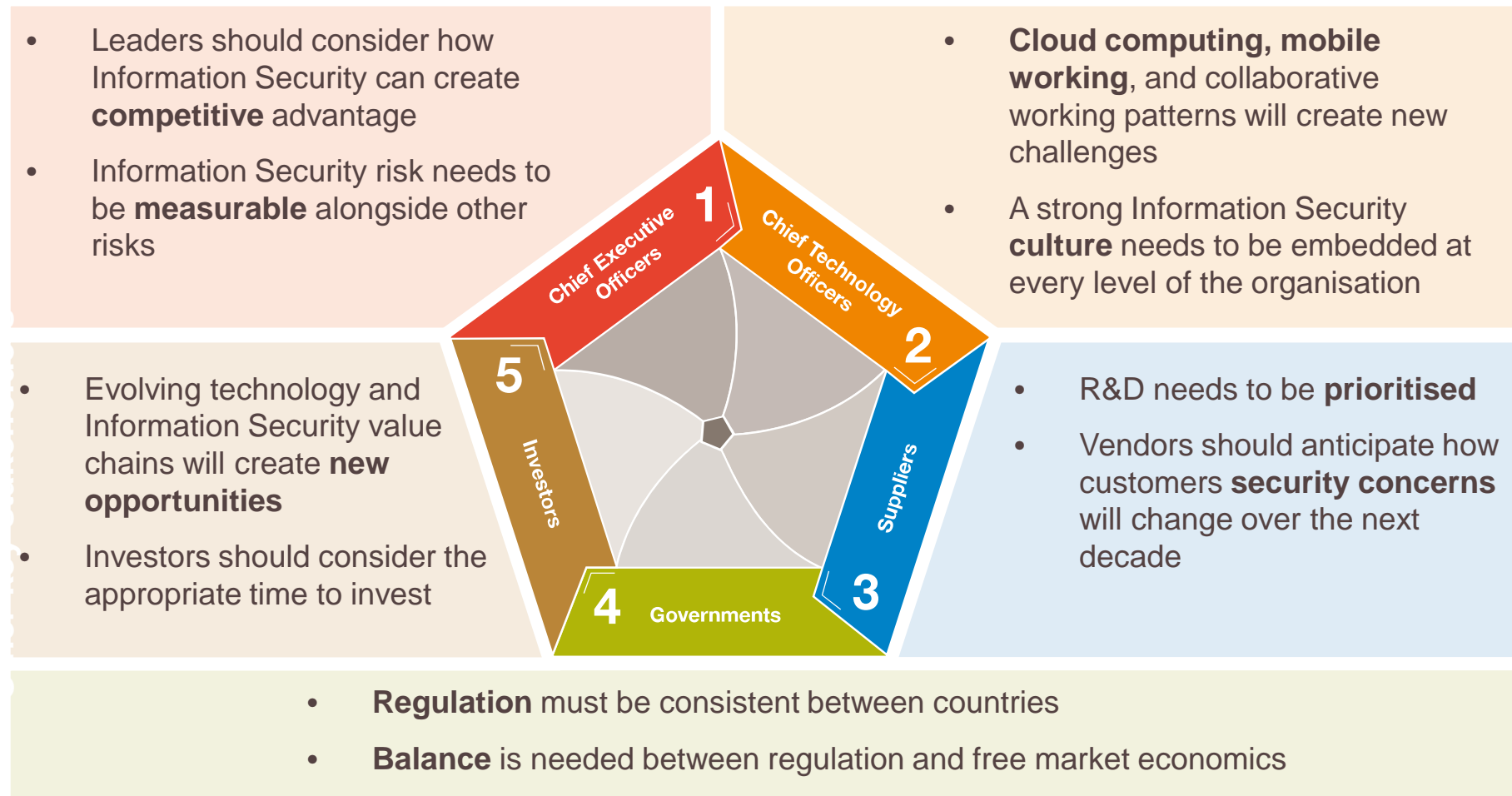
Identity and trust are key concepts to all aspects of Information Security and will be increasingly important over the next decade as:

- **The effectiveness of current identity concepts continues to decline**
- Identity becomes increasingly important in the move from perimeter to information based security
- **New models of trust develop for people, infrastructure, including devices, and data**

“ You can't just assume that an eye scan offers better protection than a username and password. The scan can still be manipulated by a hacker, who may try to switch out the master scan with their own. If you go to DNA identification, then people will get blood samples from hospitals. Every lock has a key.

James Carnell, Cyveillance ”

How will these trends impact me?



Thank you

William Beer

william.m.beer@uk.pwc.com

+44 (0) 7841 563 890

This publication has been prepared for general guidance on matters of interest only, & does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, &, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees & agents accept no liability, & disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2010 PricewaterhouseCoopers LLP. All rights reserved. 'PricewaterhouseCoopers' refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) or, as the context requires, other member firms of PricewaterhouseCoopers International Limited, each of which is a separate & independent legal entity HB 06590.