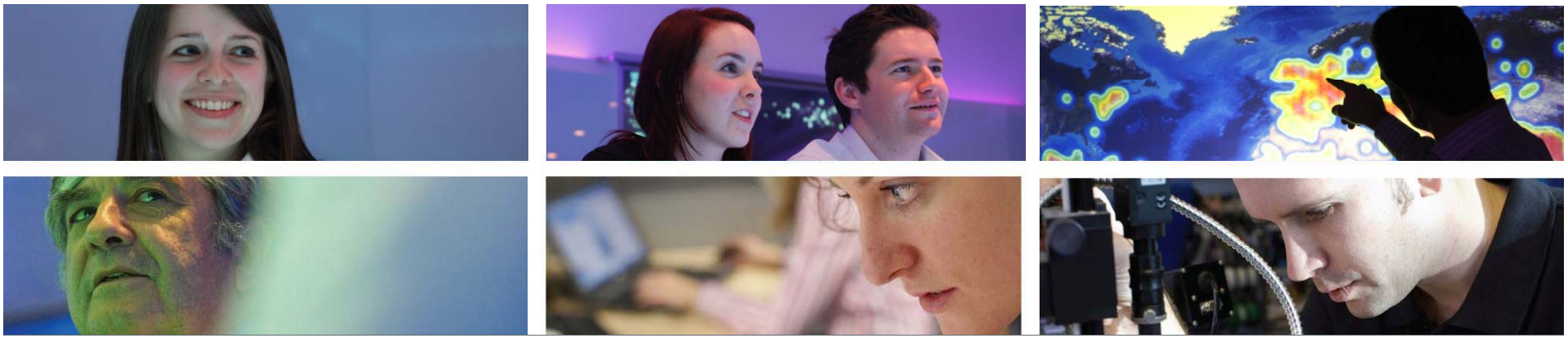
Detica

BAE SYSTEMS

CSM ACE Panel Discussion

Rationalising Security: Bringing the Dark into the Light

6th November 2012



Detica

BAE SYSTEMS

The cyber security journey

Detica

BAE SYSTEMS

Ye olden days security (up to the early 90's)

Source: Wikipedia
http://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB:Koropye_fortress_entrance.jpg

The fortress

- Only one way in and out
- Less worried about the inside
- Have a watchman who controls who can get in and out
- Not a lot of freedom for the inhabitants – everyone is on the inside

Detica

BAE SYSTEMS

The security renaissance (mid 90's – recently)

Evolution of security ideas

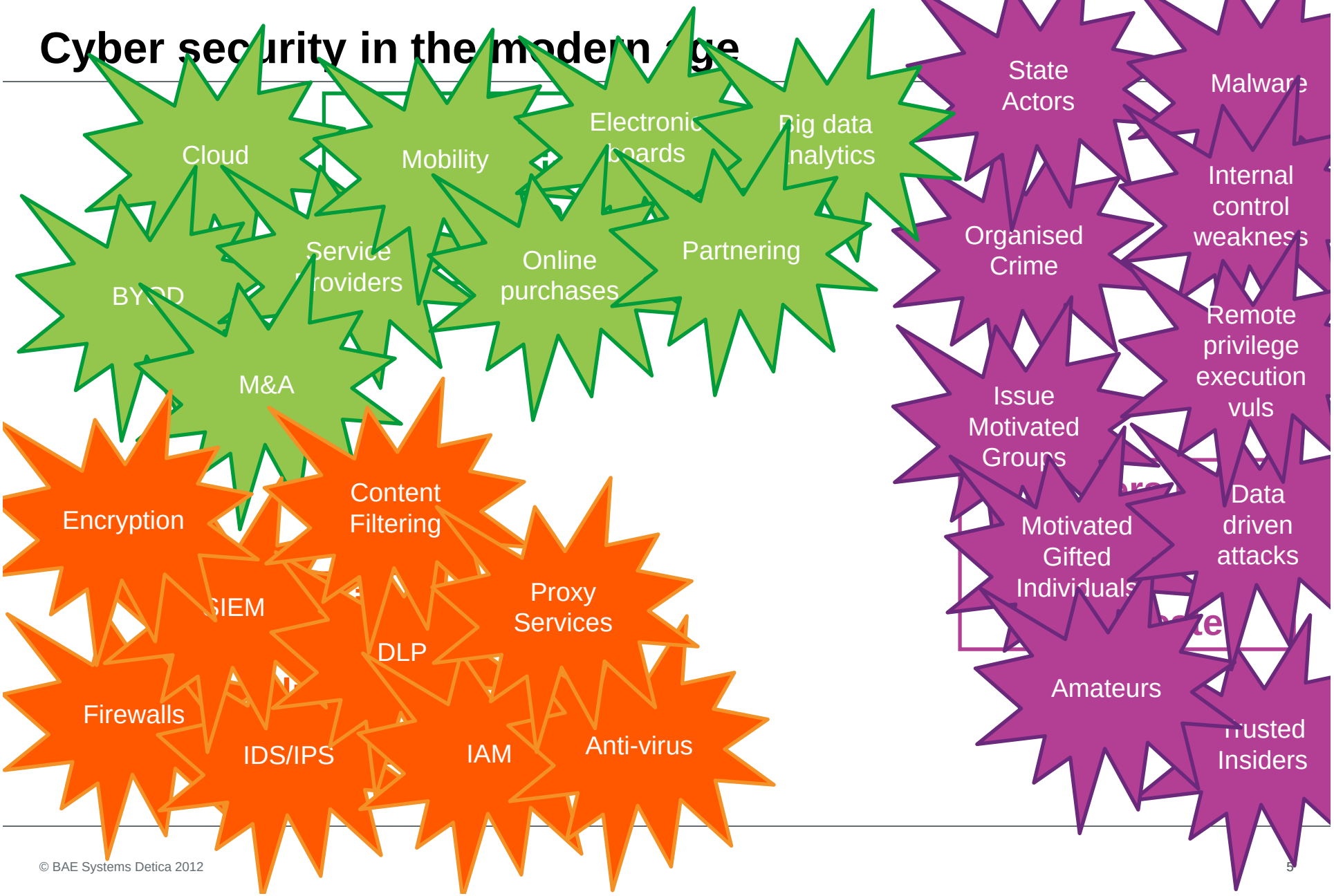
- Layers of protection
- Multiple controlled entry points
- Many more watchmen
- Still not a high degree of freedom for inhabitants
  - Although they're moving out of the castle and into walled towns with less internal restrictions

Information security became a "profession"

Detica

BAE SYSTEMS

Cyber security in the modern age



Detica

BAE SYSTEMS

Cyber security in the modern age

Business has changed in a hyper-connected world

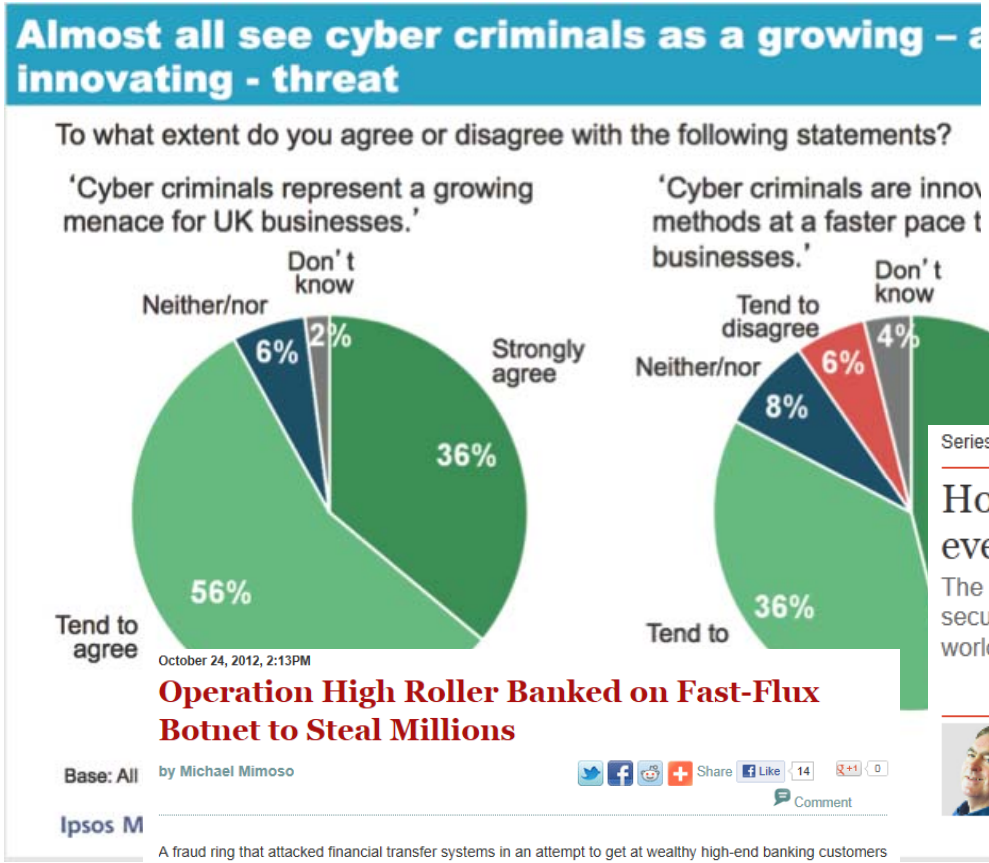
Attackers have become "highly innovative" and sophisticated

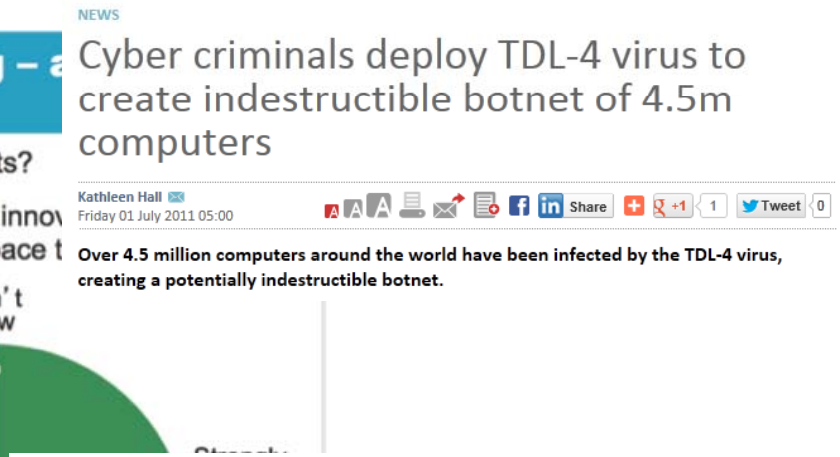
Cyber security has become incredibly complex

Detica

BAE SYSTEMS

Why our thinking must change





Detica

BAE SYSTEMS

Rationalising security

Detica

BAE SYSTEMS

What do I mean by Rationalise Security?

Web dictionary (Source *www.thefreedictionary.com/**rationalise***):

Structure and run according to rational or scientific principles in order to achieve desired results

- Experience is telling us that the current approaches aren't effective and that **attackers cannot be kept on the outside** of our networks
- An innovative and sophisticated attacker requires an **adaptive and agile defence**. We must build environments that are
  - resilient to attack
  - adaptive so that we can change quickly in response to
    - New threats
    - Changing business requirements
- In line with the theme of the CSM ACE conference, **standards and best practices can guide us** on our path to rationalising security by defining sound models for holistic security management of the enterprise

Detica

BAE SYSTEMS

What is a holistic approach?

Prepare

- Understand your
  - trophy information
  - cyber risk
  - compliance environment
  - Internal cyber capability
- Develop strategies and plans for security capabilities to address cyber risks based on priorities
- Develop cyber aware workforce and source skills as needed
- Publish your business rules for cyber security

Protect

- Design and deploy cyber security solutions to address risks and enable business to operate
  - Confidentiality
  - Integrity
  - Availability
- Apply sound engineering processes to the selection, development and deployment of cyber capabilities

Monitor

- Continually monitor systems and networks for signs of malicious activity
- Measure the effectiveness of cyber security (technical and non-technical capabilities).
- Monitor the external environment for change
- Monitor changing business requirements/emerging trends

Respond

- Have response plans and capabilities to contain and recover from cyber incidents
- Learn from cyber incidents and feedback to PREPARE processes
- Forensic capabilities to investigate cyber incidents and understand cyber threat intent

Implement an Information Security Management System