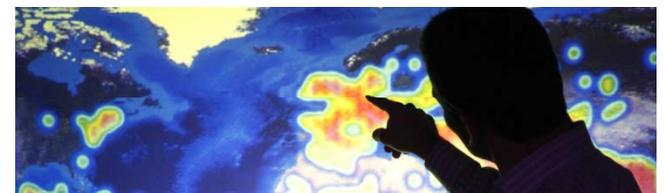


## CSM ACE Panel Discussion

### Rationalising Security: Bringing the Dark into the Light

6<sup>th</sup> November 2012



# The cyber security journey

## 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](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

## 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

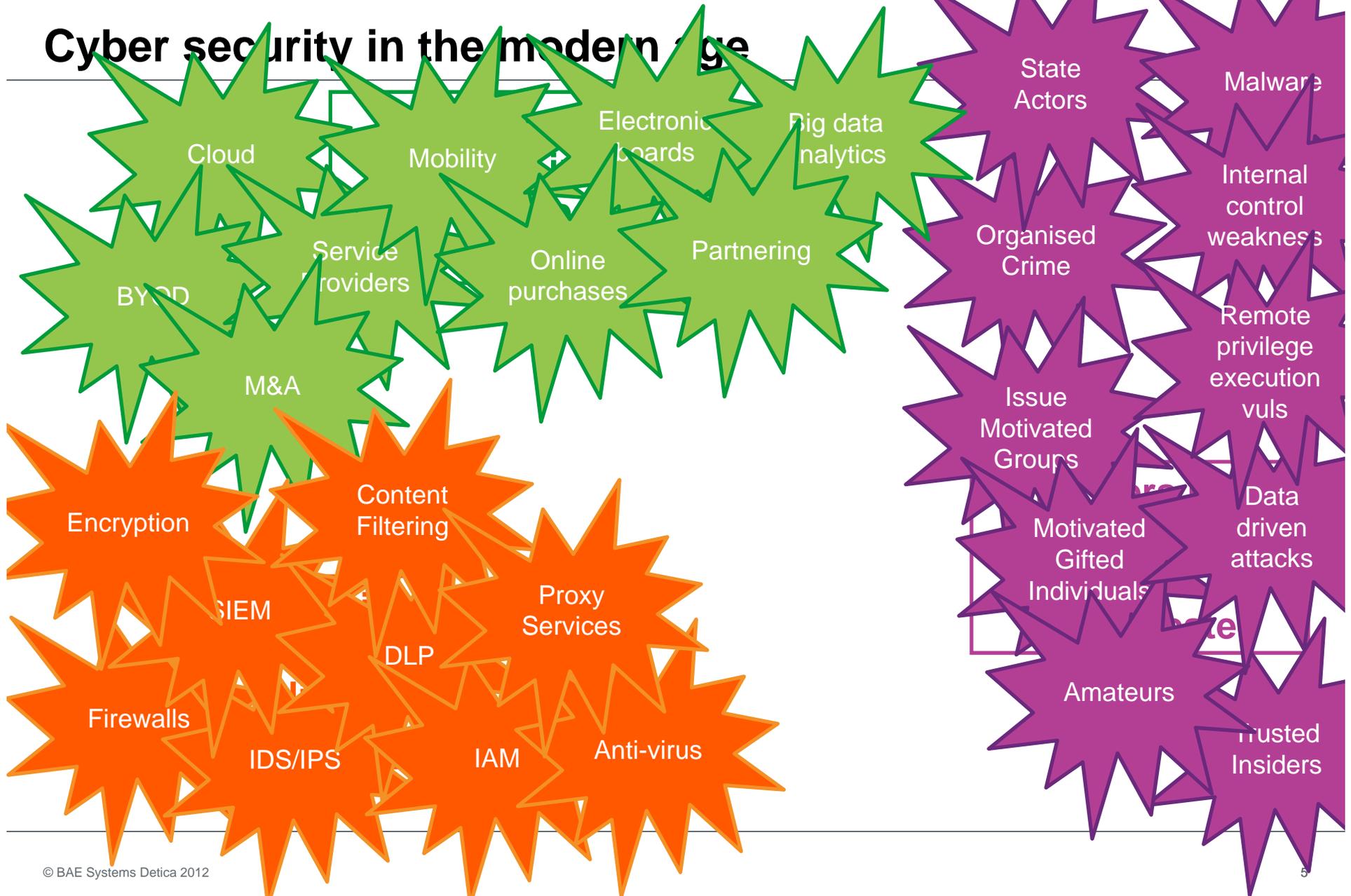
**Information security became a “profession”**

---

# Detica

## Cyber security in the modern age

BAE SYSTEMS



## Cyber security in the modern age

**Business has changed in a hyper-connected world**



**Cyber security has become incredibly complex**

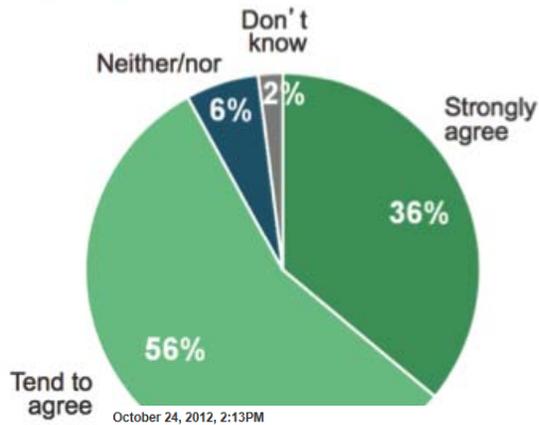
**Attackers have become “highly innovative” and sophisticated**

## Why our thinking must change

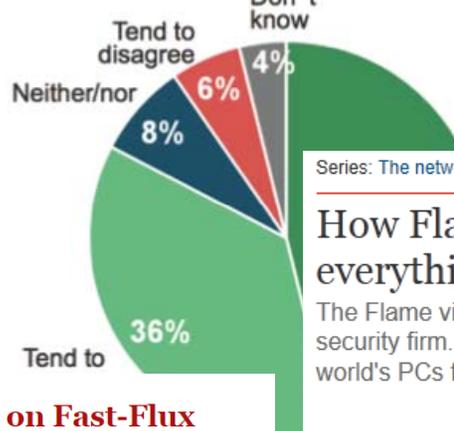
### Almost all see cyber criminals as a growing – and innovating – threat

To what extent do you agree or disagree with the following statements?

'Cyber criminals represent a growing menace for UK businesses.'



'Cyber criminals are innovating methods at a faster pace than most businesses.'



### Operation High Roller Banked on Fast-Flux Botnet to Steal Millions

Base: All by Michael Mimoso



Ipsos M

A fraud ring that attacked financial transfer systems in an attempt to get at wealthy high-end banking customers used a complicated web of malware and compromised servers in several countries to walk off with an estimated \$78 million earlier this year. While the attacks targeted financial systems, the victims seem to be limited to companies involved in manufacturing, import-export businesses, and state or local governments.

Operation High Roller was at its peak during the spring, using automated fast-flux techniques to move command and control and malware servers from host to host, using providers in the Russian city of Kemerovo.

NEWS

### Cyber criminals deploy TDL-4 virus to create indestructible botnet of 4.5m computers

Kathleen Hall  
Friday 01 July 2011 05:00



Over 4.5 million computers around the world have been infected by the TDL-4 virus, creating a potentially indestructible botnet.

Series: The networker

### How Flame virus has changed everything for online security firms

The Flame virus went undetected for two years by every online security firm. Now they need to find a new way to protect the world's PCs from malware



John Naughton  
The Observer, Sunday 17 June 2012

Jump to comments (30)

## Rationalising security

## What do I mean by Rationalise Security?

---

Web dictionary (Source [www.thefreedictionary.com/rationalise](http://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

## 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

### 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



### 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

### 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