**Don Randall MBE**
Chief Information Security Officer
Bank of England

# Measuring the future value of Security – Physical, Technical and Cyber to ensure boardroom engagement

20th November 2014
Warsaw

# Approach

- Threats
  - Terrorism
  - Cyber
  - Organised Crime
  - Fraud
  - Extremism
- Awareness
  - How
  - Who
  - When

- Technical
  - Security
  - Now
  - Future – ‘GAIT’

- Physical
  - With technical

- Cyber
- Board Room

# Physical/Technical

1. Building
    - CCTV – Facial; Behavioural; Environmental; GAIT
    - Alarms – External; Internal
    - Containment
    - Safe Havens
    - Business Continuity
    - Communications

2. Location
    - Ring of Steel

# CISO Introduction

- Why have a CISO? Investigating the structure behind the face of information security within a business
- Threat and risk: principle drivers of a CISO's establishment
- The CISO driving partnerships: gaining advantages from information-sharing without losing commercial interest

# Introduction (2)

1. General cyber threat
2. The relationship between IT infrastructure and security
3. The landscape – players – motivations
4. Partnerships
5. Communication

# Need

Federation of Small Business (FSB) recently reported:-

- Cyber crime cost its members circa. £785 million per year
- 41% of FSB members are victims of cyber crime in last 12 months
- circa 3 in 10 members have been a victim of fraud
- 20% of its members have not taken any steps to protect themselves from cyber crime

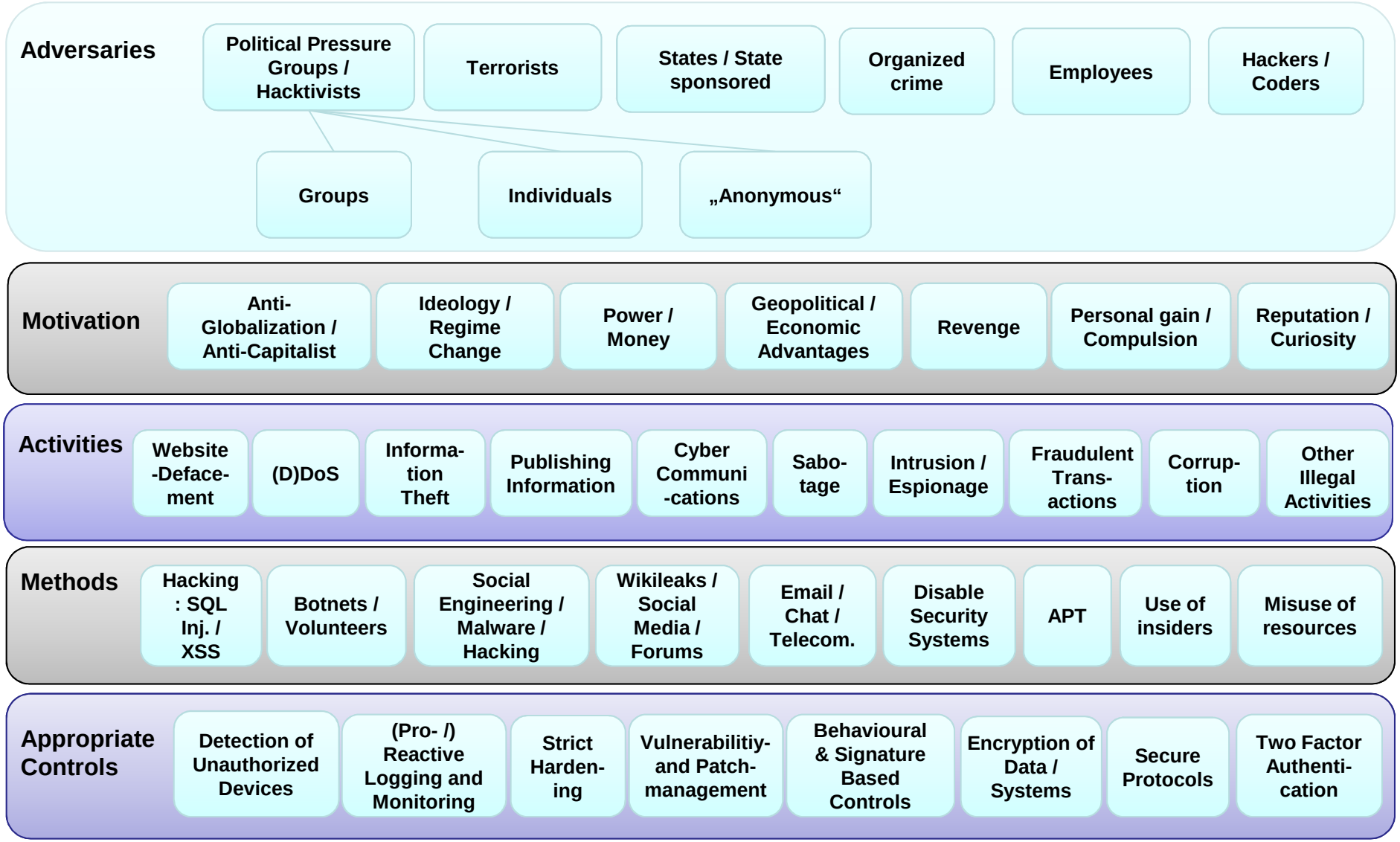
# My Personal Thoughts

*"Distinguish between Economic Cyber Enabled and Other Cyber Criminal Activity Crime"*

# Landscape – Infrastructure - Response

- Who creates landscape
- Separation/segregation between infrastructure and policing/policy
- Separate but work in harmony

# Cyber Crime – Threat Landscape



# CISO

- CISO Role
  - Technical
  - Business
  - Other
- CISO / CIO
- CISO Structure
  - Intelligence – Information – Threat Landscape
  - Investigations
  - Forensics
  - Policy
  - Education and Awareness

# Sector-wide Threat Landscape

- While Advanced Persistent Threat actors (APTs) continue to pose a systemic threat due to the potential impact that disruptive and destructive attacks may have on single organisations and the financial system as a whole, cyber-crime remains the most immediate threat for the sector. Financial institutions are impacted on a daily basis by cyber-criminals and we have observed an increasing level of sophistication in the way criminal syndicates exploit vulnerabilities to conduct large-scale financial fraud.
- Cyber-criminals are facilitated by the wide availability of malware variants that can be exchanged and purchased on the online black market. In particular, there has been an increase in the number of financial malware families designed to target online banking services and commit online banking fraud.
- UK banks have been the prime target of the sophisticated 'Shylock' malware, which has been in circulation since 2011. Around 80% of global financial institutions targeted by the malware in the last two years have been UK banks, which have suffered financial losses of millions of pounds as a result.
- Zeus is a highly effective malware tool, which has functionality to steal banking credentials whilst remaining difficult to detect / remove. First identified in 2007, its developers released the malware's source code in the public domain in 2011, spanning a number of successful variants, including Ice IX, Murofet, Citadel and the most notorious of all, Gameover.
- The concerted effort of law enforcement agencies in the UK and the US aimed at disrupting both Gameover Zeus (June 2014) and Shylock (July 2014) has arguably had a positive effect and has contributed to mitigate the threat posed by criminal syndicates controlling them in the short term.
- We are however aware of new variants of the Gameover Zeus malware currently emerging that may prove to be more difficult to disrupt. For the time being, the creators of this new malware strand are believed to be focusing on rebuilding the necessary infrastructure in preparation for resuming their criminal activity.
- One of these variants which has recently been observed affecting UK organisations is Cridex/Dridex. In addition to targeting online banking activity, the malware could potentially also be used to target Bacs/FPS payments systems. To date, there have been no confirmed instances of compromise of Bacs payment systems via Cridex/Dridex. However, in early August, a number of European financial and government institutions, including several UK banks and government departments, were targeted by a phishing campaign that was designed to drop and exploit this malware. Although the attack was unsuccessful, the large number of organisations affected was in itself significant and would suggest that the threat posed by this malware family and those who control it may grow in the near future.

# Information-sharing And Private-public Sector Engagement

- Participation in a number of initiatives and partnerships designed to facilitate and improve cyber threat information-sharing between government and law enforcement agencies and the industry. These include:
- The **National Cyber Crime Unit** within the **NCA** has recently set up a number of groups to encourage and facilitate engagement with the sector in the fight against cyber-crime in the UK. The Bank is an active member of the NCA's Industry Working Group and Criminal Marketplace Threat Group and is looking to engage on a number of additional topics, such as crypto-currency. Following the agency's intention to assess the impact of recent law enforcement campaigns that disrupted the Gameover Zeus and Shylock malware, the Bank volunteered to act as main point of contact to collect and provide feedback from the industry.
- The NCA also hosts the **Information Sharing Group**, a Home Office initiative designed to promote information sharing between the government and the financial sector. The group will mainly focus on anti-money laundering, assets recovery and emerging economic threats. However, it was proposed that cyber should be included as an additional work-strand.
- In April, the Home Office Breakfast Meeting  was held which was designed to foster joint discussion and closer collaboration between the government, law enforcement and the sector to increase the resilience of the financial sector to threats from serious and organised crime.
- **CERT-UK** (Computer Emergency Response Team): tasked with leading the response to any cyber-attacks of national significance, its key objective is to improve the UK's cyber incident response arrangements and extending them beyond the CNI to include the wider UK economy. CERT-UK is a long overdue part of the cyber defence landscape, and is an important initiative. Its lack of investigative powers is a potential weakness, and it will be dependent on other bodies to take action, but it should provide much needed co-ordination in major cyber incidents.
- **CISP** (Cyber Security Information Sharing Partnership): UK Government initiative to facilitate real time cross-industry information sharing on cyber threat and vulnerabilities.
- **FSIE** (Financial Services Information Exchange): CPNI-led initiative where organisations who are considered critical to financial system are able to share sensitive information in a trusted environment.
- **CSIG** (Cyber Security Information Group): informal intelligence-sharing group for UK financial organisations. There are currently around 15 organisations that are recognised CSIG members.
- **FS-ISAC** (Financial Services Information Sharing and Collaboration): US-focused finance sector not-for-profit group. It also serves as the sector communications hub during emergencies through the delivery of rapid notifications and communications to and among its 4400 members. Last year, an **FSISAC-EU** group was launched to facilitate increased sharing and co-operation in the region.
- **NCFTA** (National Cyber Forensics Training Alliance): a partnership grouping based in Pittsburgh, whereby industry, law enforcement and academia have brought their resource together to investigate and disrupt cyber-crime.

# Partnership Introduction

- Threats
- Realities (lone actors)
- Partnerships
- Fast time – accurate and authoritative
- Civil unrest
- Communication is key

# History – Public/Private Partnership

| | |
|---|---|
| 1980's | Neighbourhood Watch |
| 1990 | More Refined "Sister Banks" |
| 09/11/01 | Need |
| 2004 | Project Griffin |
| 2012 | CSSC |

# The Risks

- Terrorism – local – national – international
- Cyber crime – economic – infrastructure
- Natural disaster
- Employee issues
- Civil Unrest
- Insider Threats

# Private & Public Sector Security Harmonisation

BENEFITS

Extra Eyes, Ears & Minds

MEASUREMENTS OF SUCCESS

Positive Results

QUANTUM LEAPS

Officially Sharing

Two way Interactive Street

Fast Time, Accurate Authoritative

Concept to Reality – No Failure – No Miss Use

Total Trust and Expectation

# Private & Public Sector Security Harmonisation - Examples

Sister Banks – Global

Project Griffin

- London - All London Boroughs plus Olympics
- UK Nationwide
- Scotland
- Australia
- New York
- Canada
- South Africa
- Singapore
- India
- United States

“Internationally Transferable”

# The Community

- Small / Medium Enterprises (SMEs)
- The Wine Bar / Kiosk / Shop
- “Henry’s Coffee Shop”
- How does it help

# Working Together

- Share what you do wrong
- Partnerships – ‘Sister Banks’ – Project Griffin
  - Champions
  - Private / Public
  - Private / Private
  - Public / Public
- Law Enforcement / Private Sector

# Working Together

- Who do you engage?
- How do you share?
- When do you share?
- Dealing with Bureaucracy
- Formal versus informal

# Project Griffin

- How conceived
- Champions
- Make it happen – No Showstoppers - Problems
- Three Strands – Flexibility
- Measurables
- Expansion
- Congealing current initiatives

# Current Status – Project Griffin

- Over 40,000 London guards attended awareness day
- In excess of 2,000 buildings covered
- In excess of 1 Million people better supported
- Griffin CVIT
- Griffin fraud
- Griffin ASBO

# CSSC Aim

To provide and facilitate for UK business to be safety and security aware, by improving communication between the public and private sector on security matters and creating a legacy of improved communication and awareness.

# CSSC Creation

- 40 Disciplines (ISL's)
- Model Works
- Bank of England Facilitate
- 30 minutes SLA, Message distributed – 8.5 million recipients

# Industry Sectors

**ACADEMIA**

Association of Colleges
Association of University Chief Security Officers

**ACCOUNTANCY (Professional Services)**

PwC Informal Network

**BANKING**

Sister Banks
British Bankers Association
Building Societies Association
FaceWatch

**BUSINESS REP ORGANISATIONS/ GEOGRAPHICAL**

London First

CBI( Confederation of Business Industry)

FSB (federation of Small Business)

LCCI (London Chamber of Commerce and Industry)

**CONSTRUCTION**

Laing O'Rourke Informal Network

**DEFENCE**

Lockheed Martin / ADS (UK Aerospace, Defence, Security and Space industries.) Informal Network

**ENERGY**

Electricity Security Managers Forum

**FOOD & SUPPLY CHAIN**

Food and Drink Security Association

**HOTELS**

Institute of Hotel Security Managers

British Hospitality Association

Informal Hotel Security Network

**INFORMATION TECHNOLOGY**

**INSURANCE**

Insurance Security Network

**LAW**

Berwin Leighton Paisner Informal Network

**MEDIA**

BBC, NBC Informal Network

**NIGHT TIME ECONOMY**

Mitchells and Butlers Informal Network

**PETROCHEMICAL**

Petrochemical Security Network

**PHARMACEUTICAL**

Pharmaceutical Industry Security Forum

**POST OFFICE**

Royal Mail

Grapevine Community

**PROPERTY MANAGEMENT**

Royal Institute of Chartered Surveyors

**RETAIL**

British Retail Consortium

**SECURITY**

British Security Industry Association
ASIS, IPSA, SIA, Security Institute

**SPECIALISTS**

Overseas Security Advisory Council
International Security Management Association
European Corporate Security Association
Risk and Security Management Forum
National Counter Terrorism Security Office
Centre for the Protection of National Infrastructure

**TRANSPORT**

Transport for London
Road Haulage Association
Freight Transport Association

**TRAVEL**

Association of British Travel Agents
Civil Aviation Authority
Tour Operators

**TELECOMS**

Telecommunications UK Fraud Forum

**TOURISM AND LEISURE**

Museum and Galleries
public Leisure Centres

**LONDON BOROUGHS & RESILENCE**

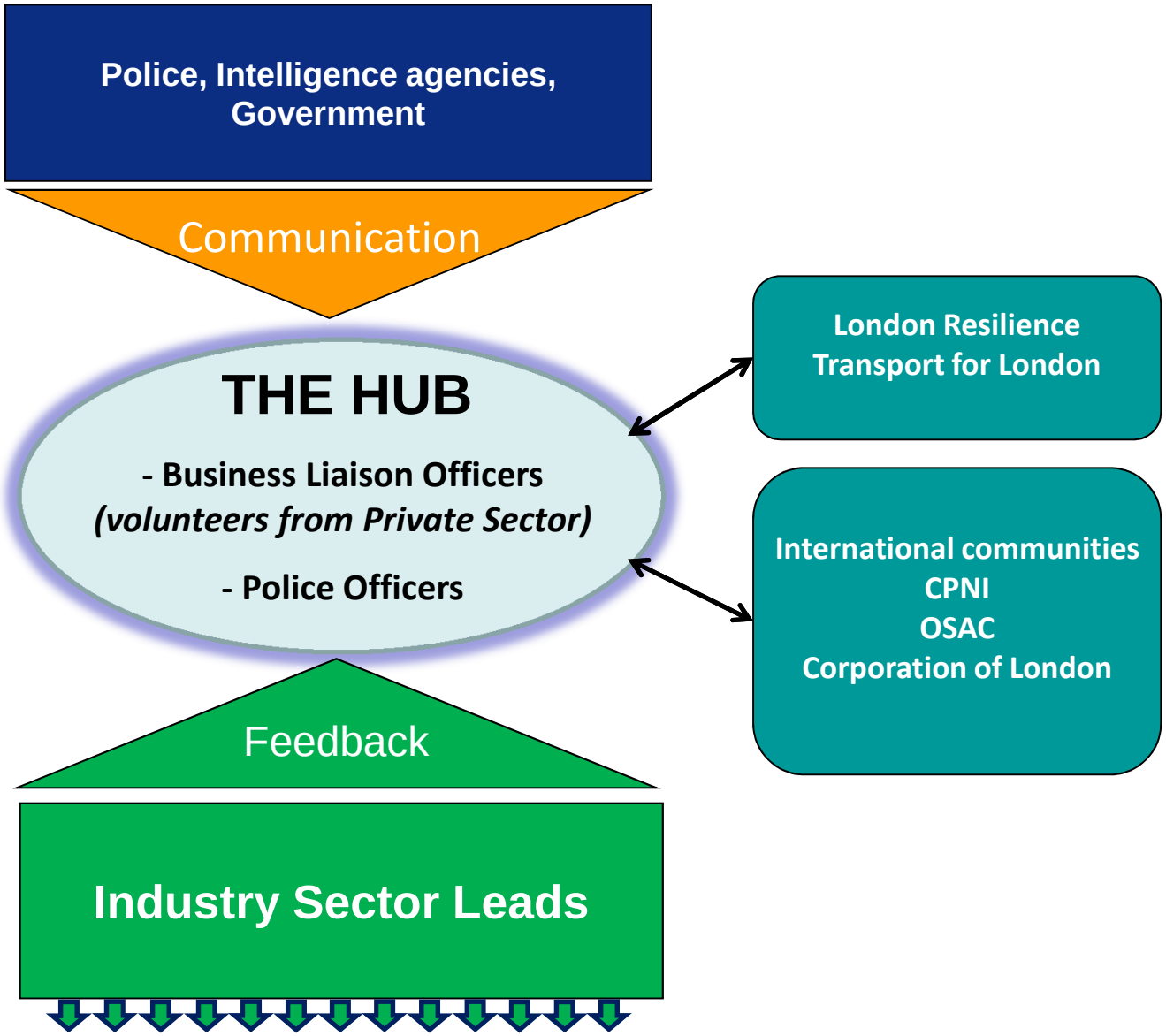
London Resilience Team

**NEIGHBOURHOOD LINK**

# Communications Framework

**Methods of Communication**

- Bridge / conference call
- Newsletter
- Email
- Website
- Other



# ISL role in CSSC

- 60 plus Industry Sector Leads representing 40 sectors
- Appointed by sector & agreed with MPS/Home Office
- Organise sector members & broaden and recruit if gaps
- Keep lists current ensure hub understand sector reach
- Establish sector cascade capability
- Contribute resources and headcount to partnership hub
- Represent sector on bridge calls
- Cascade core messages to sector members
- Coordinate and escalate business needs and concerns
- Three ISL workshops/events per year

# Benefits of CSSC to Business Sector

- Connects, builds and enhances proven public/private partnerships
- Accurate fast time and authoritative communications
- Cut ‘n’ paste communications
- Two way flow of communications
- Sector specific when necessary
- Significant added value to risk management
- Vital added value to crisis management

# Achievements

Anecdotal

- Tasking – London First
- Sir David Veness – We can do it
- Buckets, Pyramids, ISL’s
- Hotel Stats
- PISF – Stats and Story
- James Hill – ARL’s
- Pre Olympics
- Tamils, Hotel, Finance
- Olympics Every Day
- The Fire Incident

# United / Partnerships

- Government
- Law Enforcement
- Preventative Initiatives
- Griffin – Sister Banks, RSMF et al
- Public/Private Sector
- Fast Time – Accurate - Authoritative

# Benefits of CSSC

- Key communication tool to increase our ability to warn and inform business and the wider public in London and further afield
- Helped build a greater relationship with the business community in London
- Strengthens work of the Business Sector Panel
- Enhances and expands our situational awareness

# Legacy

- Structure: MPS/ City / Volunteers / BoE Office
- Charity:  £30k Sponsorship
- August 2013 – June 2014:  UK Cities
- Commonwealth Games June 2014

# Conclusion

- The issues do not change, only the methodology
- The counter measures need to be understood and fully exercised
- Partnership is the only way to succeed

“Lets Work Together”

“Comfort Builds Complacency”