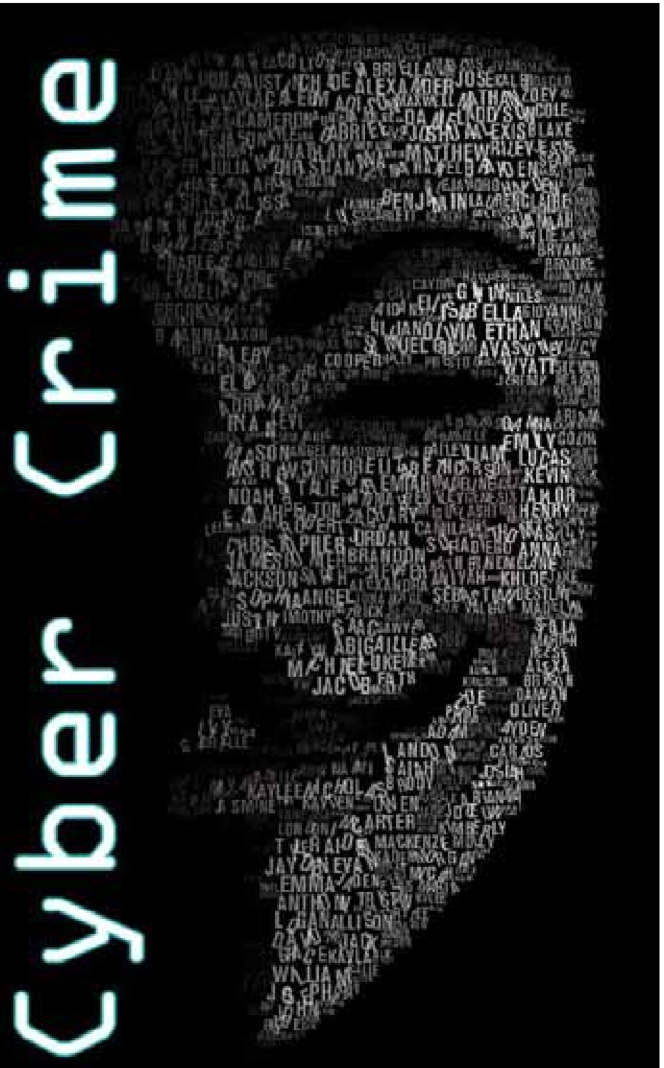
Cyber-Security – UK / European Experience

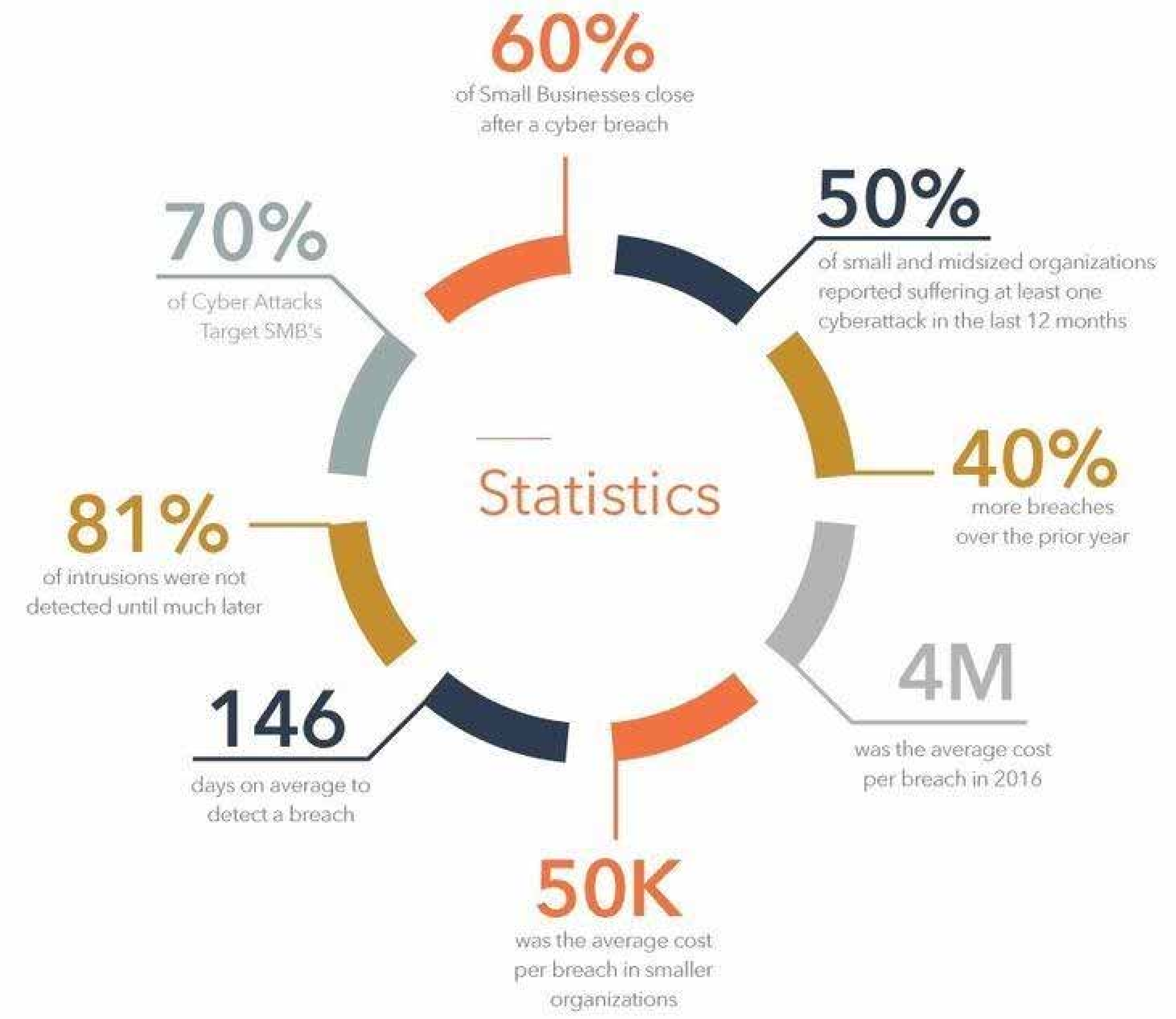
Jon Murthy

ILAC and IAF Communications Chair

What’s at risk?

- Data theft
- Corporate hacking
- Critical infrastructure
- Smart grid
- Smart manufacturing
- Smart cities
- Smart homes
- Internet of things
- Transport systems
- And so on….





Statistics

60%
of Small Businesses close after a cyber breach

50%
of small and midsized organizations reported suffering at least one cyberattack in the last 12 months

40%
more breaches over the prior year

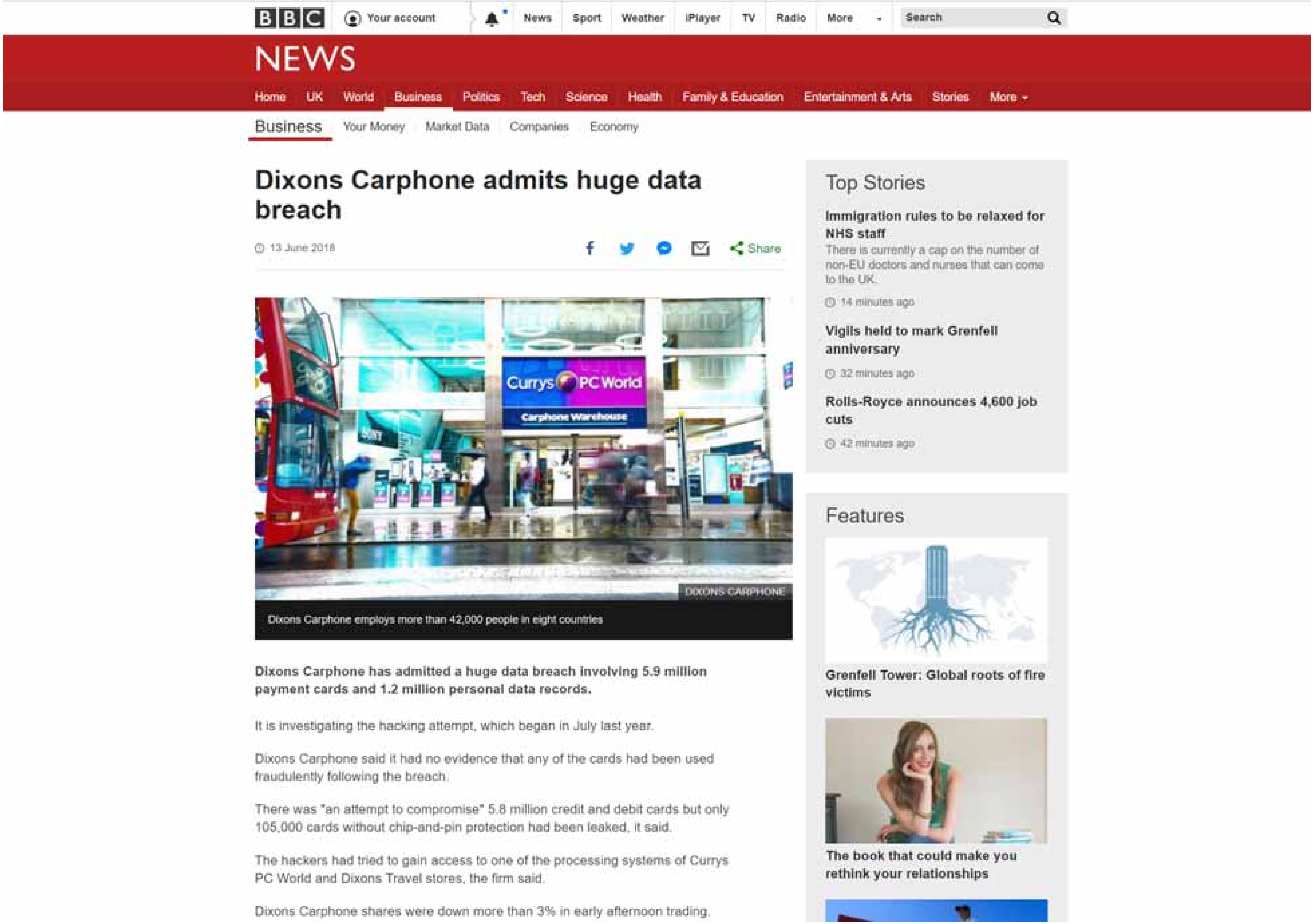
4M
was the average cost per breach in 2016

50K
was the average cost per breach in smaller organizations

146
days on average to detect a breach

81%
of intrusions were not detected until much later

70%
of Cyber Attacks Target SMB's



Dixons Carphone admits huge data breach

13 June 2018

Dixons Carphone employs more than 42,000 people in eight countries

Dixons Carphone has admitted a huge data breach involving 5.9 million payment cards and 1.2 million personal data records.

It is investigating the hacking attempt, which began in July last year.

Dixons Carphone said it had no evidence that any of the cards had been used fraudulently following the breach.

There was "an attempt to compromise" 5.8 million credit and debit cards but only 105,000 cards without chip-and-pin protection had been leaked, it said.

The hackers had tried to gain access to one of the processing systems of Currys PC World and Dixons Travel stores, the firm said.

Dixons Carphone shares were down more than 3% in early afternoon trading.

Top Stories

Immigration rules to be relaxed for NHS staff

There is currently a cap on the number of non-EU doctors and nurses that can come to the UK.

14 minutes ago

Vigils held to mark Grenfell anniversary

32 minutes ago

Rolls-Royce announces 4,600 job cuts

42 minutes ago

Features

Grenfell Tower: Global roots of fire victims

The book that could make you rethink your relationships

Why is it important to organisations?

- Reputational damage
- Share value
- Customer trust
- Financial penalties
- Mitigation costs
- Marketing costs?

The cost of breaches

- Breach of 157,000 customers
- £400,000 fine
- Loss of 101,000 customers
- 11% share price drop
- Remediation costs
- Total ~ £80m

Current landscape – cyber-security activities

- Standards with cybersecurity elements
- > 1000 standards found
- > 50 Standards making bodies

The current issues

- Multiple standards and approaches
- Different national regulatory responses to the market needs for cybersecurity
- Sector and market need differs

For example…

- Industrial Automation System
  - Many components
  - In confined physical area
- Railway System
  - Many components
  - Spread over a large physical area

UK experience

- Take up of standards / CA is low
- **59** laboratories accredited for IT Security Testing
- **3,367** companies with ISO 27001
- Government is less supportive of ILAC / IAF recognised accredited CA
- No clear policy

UK experience

- Basic entry level scheme
- Backed by Govt, Business and Insurers (incentives)
- National Cyber Security Centre (NCSC – part of GCHQ) operates its own accredited certification programme
- 5 Accreditation bodies, 170 Certification Bodies
- Oct 2014 – must be certified to bid for Govt contacts involving personal data
- Not suitable for UKAS accreditation

National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

UK experience

- Cyber Essentials uses the term ‘accreditation’ yet it is tick box
- UKAS is seeking to revamp scheme and combine with ISO 27001.

National Cyber
Security Centre
a part of GCHQ

CYBER
ESSENTIALS

UK experience

National Cyber Security Centre
a part of GCHQ

Scheme

Common Criteria

Created: 03 Sep 2015
Updated: 01 August 2016

- UKAS accredits NCSC as a CB for Common Criteria scheme
- UKAS also accredits 4 Commercial Evaluation Facilities (testing labs) who feed into scheme.
- Scheme provides formal recognition of a developer's claims about the security features of their product.
- **1864** certs in Europe

European experience

- Recognise the value of accredited certification schemes – security of systems and digital technologies
- ENISA identified fragmentation between economies / challenges to interoperability.

European Commission

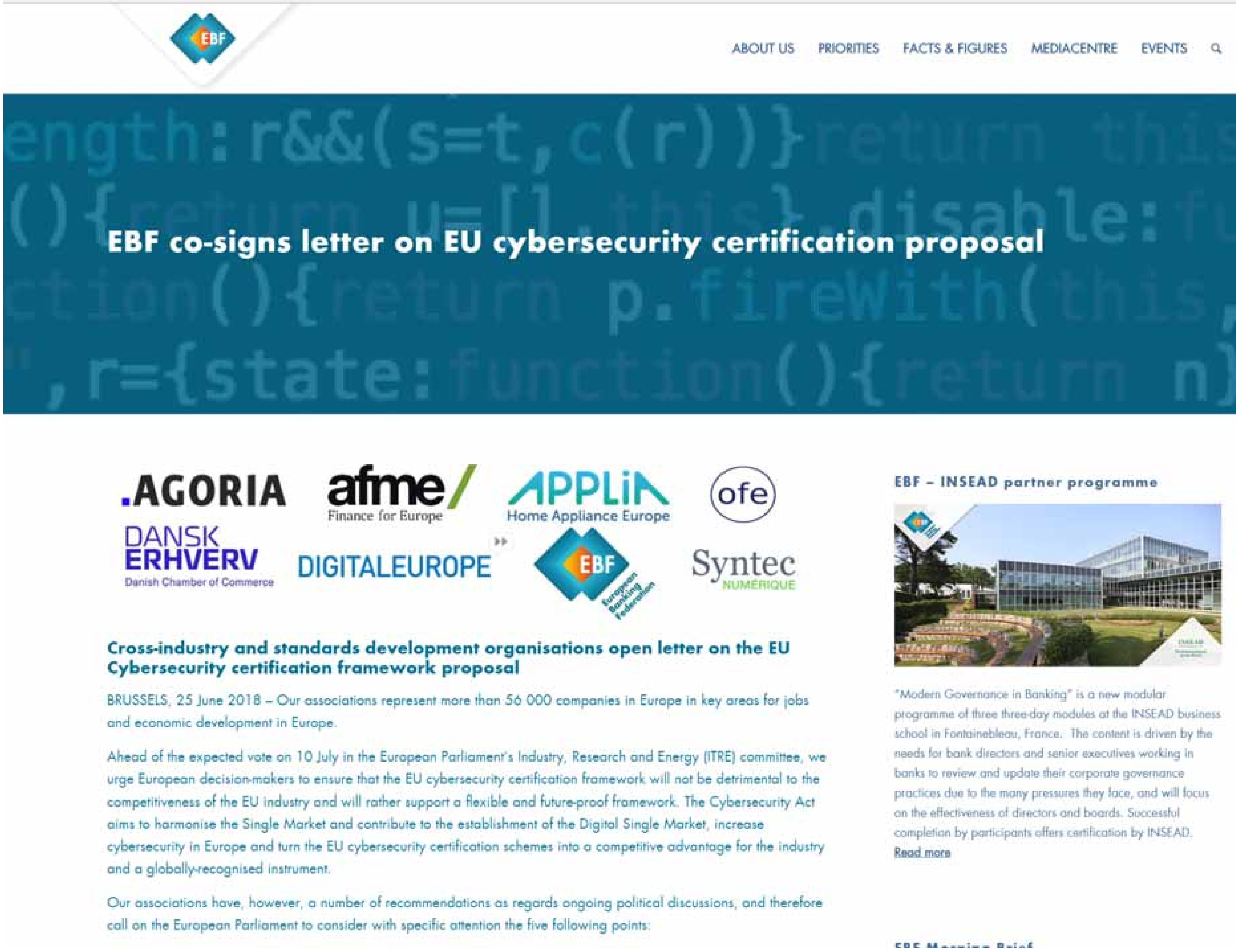
European experience

- Driven by NIS Directive, GDPR , the eIDAS Regulation and the Revised Directive on Payment Services – need for trustworthy IT systems
- The EU is reforming ENISA to:
  - Increase the **trust and security** of ICT products and services
  - **Harmonise** the existing certification landscape to reduce costs and administrative burdens for companies
  - Progress the **Digital Single Market**

enisa
European Network
and Information
Security Agency

European experience

- To coordinate the governance, aligning the development of certification schemes and providing a single source of authorisation
- New ENISA Reg will require that organisations certifying EU cyber security schemes must be accredited by the national accreditation body in line with the requirements of Regulation 765/2008.



EBF co-signs letter on EU cybersecurity certification proposal

.AGORIA
afme/ Finance for Europe
APPLiA Home Appliance Europe
ofe
DANSK ERHVERV Danish Chamber of Commerce
DIGITALEUROPE
EBF European Banking Federation
Syntec NUMÉRIQUE

Cross-industry and standards development organisations open letter on the EU Cybersecurity certification framework proposal

BRUSSELS, 25 June 2018 – Our associations represent more than 56 000 companies in Europe in key areas for jobs and economic development in Europe.

Ahead of the expected vote on 10 July in the European Parliament's Industry, Research and Energy (ITRE) committee, we urge European decision-makers to ensure that the EU cybersecurity certification framework will not be detrimental to the competitiveness of the EU industry and will rather support a flexible and future-proof framework. The Cybersecurity Act aims to harmonise the Single Market and contribute to the establishment of the Digital Single Market, increase cybersecurity in Europe and turn the EU cybersecurity certification schemes into a competitive advantage for the industry and a globally-recognised instrument.

Our associations have, however, a number of recommendations as regards ongoing political discussions, and therefore call on the European Parliament to consider with specific attention the five following points:

EBF – INSEAD partner programme

"Modern Governance in Banking" is a new modular programme of three three-day modules at the INSEAD business school in Fontainebleau, France. The content is driven by the needs for bank directors and senior executives working in banks to review and update their corporate governance practices due to the many pressures they face, and will focus on the effectiveness of directors and boards. Successful completion by participants offers certification by INSEAD. Read more

EBF Morning Brief

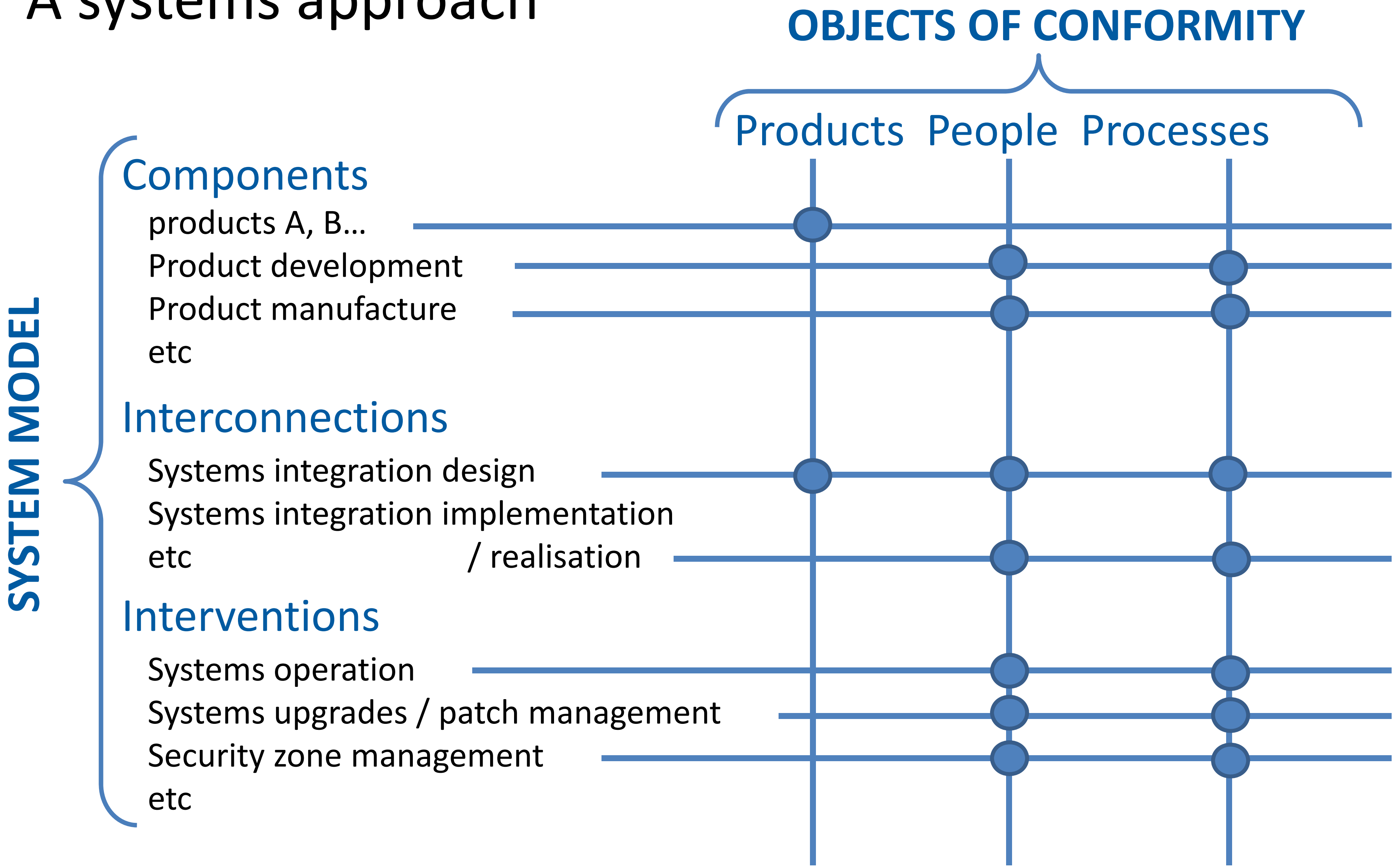
European experience

- Certification should be **voluntary**
- Conformity assessment methods and requirements should be **defined in the schemes and not in the regulation** itself.
- Industry **consultation**
- The adoption of the schemes should include a process to ensure that they are aligned or could take part in existing **international mutual recognition** agreements to ensure that the EU certificates are globally recognised.
- Reference to **global standards** should prevail.

UNECE and IEC proposal - Macro view

- The systems that concern us for the issue of cybersecurity are made up of:
    - Components (physical or virtual)
    - Interconnections (systems integration)
    - Information flow
    - Interventions (human, virtual or automatic)
- Best cybersecurity = world's best practices (eg: international standards) applied in a systems-approach, supported by appropriate CA.

A systems approach

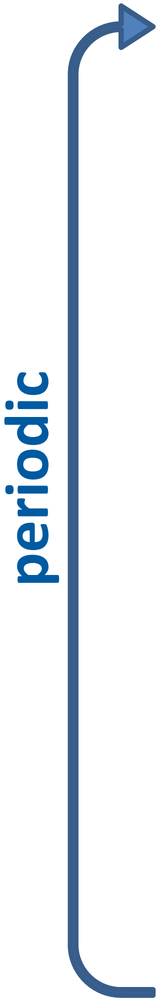


OBJECTS OF CONFORMITY

SYSTEM MODEL

SYSTEM MODEL	Products	People	Processes
Components			
products A, B…	●		
Product development		●	●
Product manufacture		●	●
etc			
Interconnections			
Systems integration design	●	●	●
Systems integration implementation / realisation		●	●
etc			
Interventions			
Systems operation		●	●
Systems upgrades / patch management		●	●
Security zone management		●	●
etc			

A systems approach



1) Map sector application to generic matrix model
2) Risk analysis of sector application map
   - Identify and rate risk points
3) Determine appropriate level of CA for each risk point according to risk level rating
4) Identify requirements documents (standards)
   - Determine what is available/appropriate
     → standards gap analysis
   - Determine how to fill the gaps – SD
5) Apply appropriate CA to appropriate standards at each risk point

Review, revise, renew

Next steps

- Validate the Generic Matrix Model (GMM) approach
- Obtain sector-specific GMM
  - Critical infrastructure (Oil/gas, Nuclear, Electric grids, etc)
  - Railways
  - Cloud computing
  - Smart energy
  - Smart factory
  - Smart buildings
- Develop risk analysis and ranking methods

Concluding points

- Need for rationalisation
- Cyber-security issue needs to be developed globally, not national or regional (based on international standards)
- It requires a systems approach - not only technical (products, systems, design), management processes or personal competencies – but all three
- It requires an understanding of the system to be protected
- It requires risk analysis and rating to determine right level of CA
- Appropriate requirements are placed at the 'risk' points

www.publicsectorassurance.org

For further information

iaf.nu | ilac.org

@IAF_Global @ILAC_Official

Jon Murthy
T: +44 781 8570075 **| E:** jm@ukas.com

www.youtube.com/user/IAFandILAC

www.publicsectorassurance.org/

www.business-benefits.org