Building-in Cyber Security, Usability and Inter-Operability

Paul Kearney

paul.Kearney@bcu.ac.uk

BIRMINGHAM CITY University

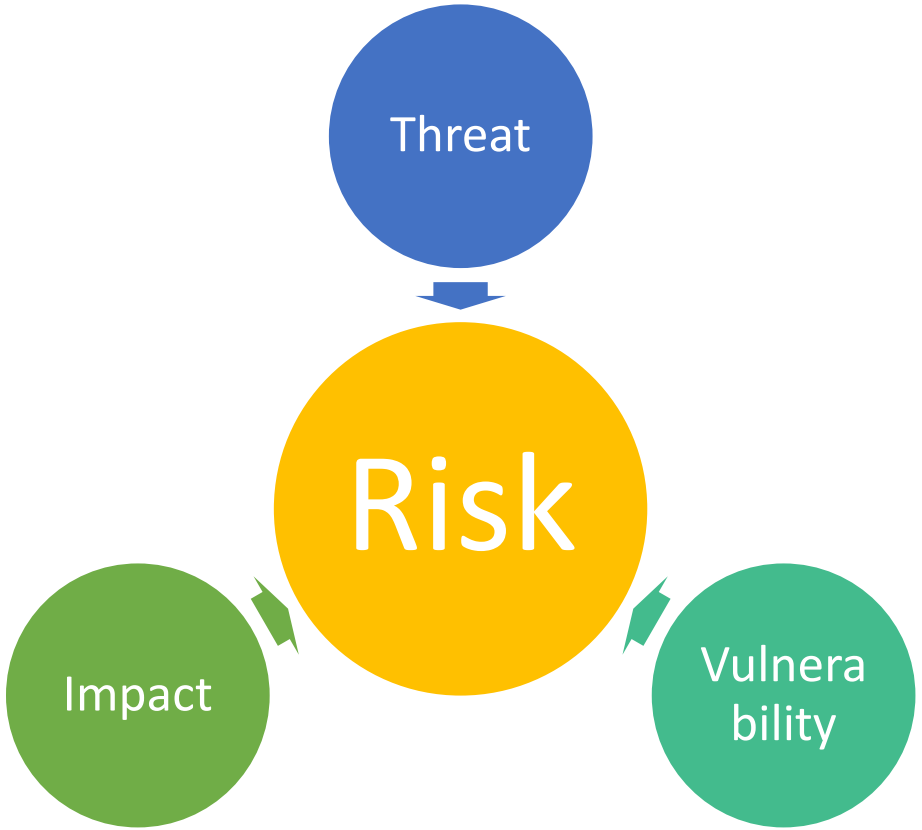
Paul Kearney

- Education:
  - BSc in Mathematical Physics from University of Liverpool
  - PhD in elementary particle theory from University of Durham
- Employment:
  - 10 years at BAe Military Aircraft, Warton, Lancashire
  - 7 years at Sharp Laboratories of Europe, Oxford
  - Nearly 20 years at BT, Adastral Park, Martlesham Heath, Ipswich. Currently Chief Researcher in the Security Futures Practice, Research and Innovation.
  - Professor of Cybersecurity (part-time) at BCU since November 2015.
- External activities include:
  - Member of H2020 Protection and Security Advisory Group
  - On steering board of European Cyber Security Organisation WG6, Strategic Research and Innovation Agenda
  - Contributor to IoT Security Foundation and prpl Foundation WGs

Main points

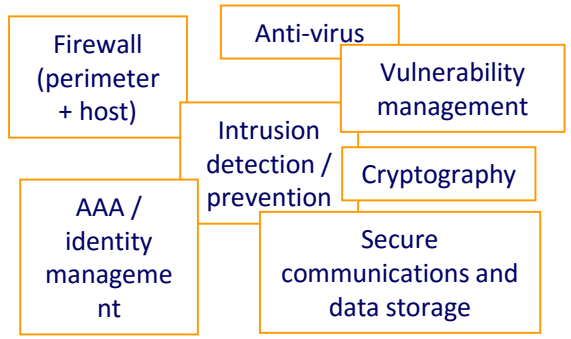
- Digital technology offers many benefits, but also brings danger for the unwary
- Concerns about cyber-security are one of the main pacing factors governing the rate of digital innovation, including
  - Virtualisation and cloud computing
  - Big data and intelligent analytics
  - Internet of Things and Smart ‘X’
    - X = Cities/Health/Transport/Manufacturing/Transport …
- There are no secure systems!
  - Risk-led approach combining protection, detection, response and recovery
  - Recognise organisations as socio-technical systems – see people as part of the solution, not part of the problem
  - Co-operation and intelligence sharing

Security is about managing risk … making decisions about an uncertain future.



Cost vs benefit

Cost of controls:

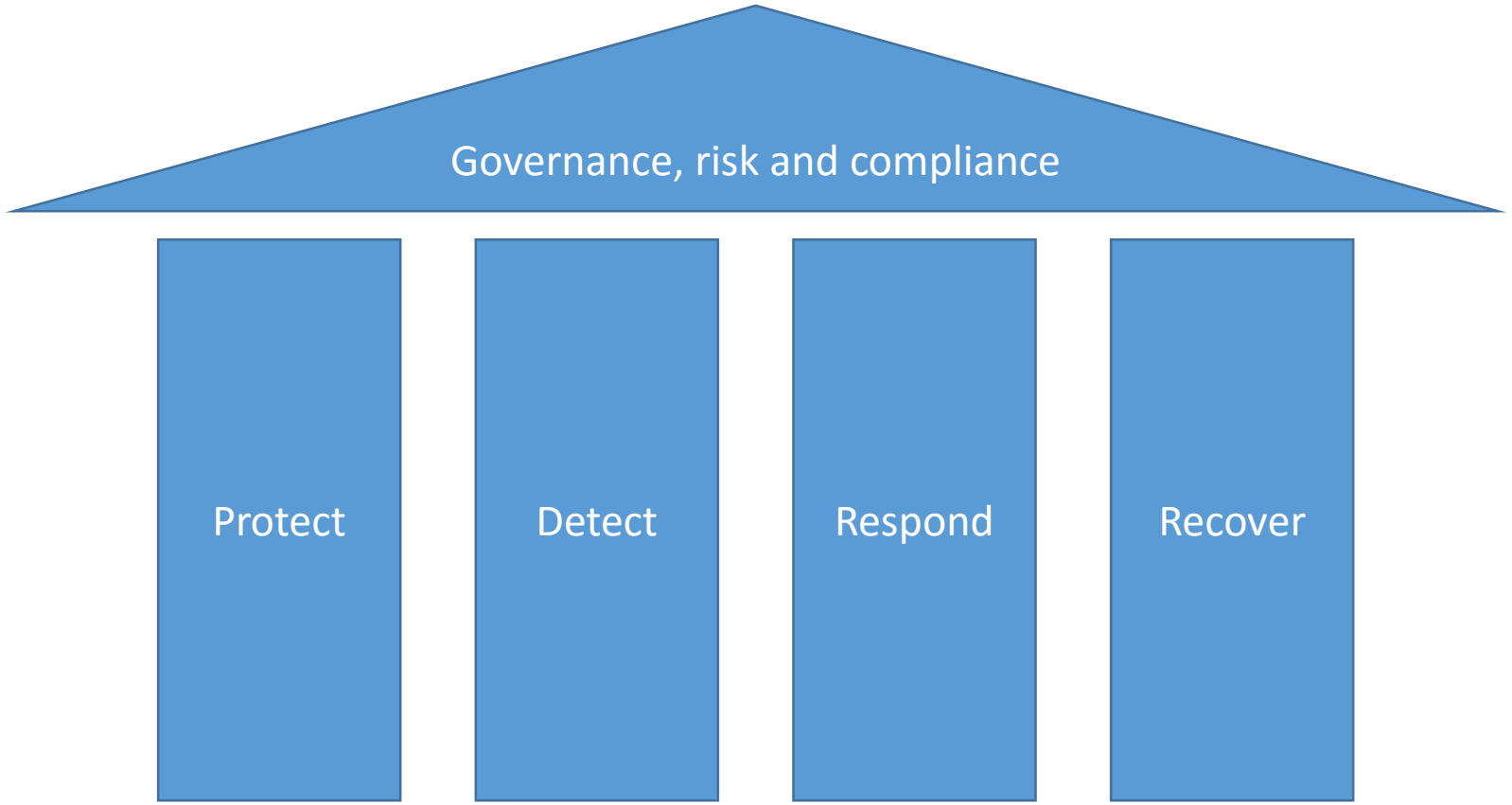


Reduction of risk to assets:

- Money
- Equipment / physical assets
- Data and software
- Information and knowledge
- Reputation, trust
- Business operations
- Time
- Personal information (privacy)
- Copyright
- People (family, children, employees)

- Security ‘controls’ reduce risk, but have costs of reduced functionality and/or convenience.
- Ideal solution balances risk and cost for customer. Highly subjective!

The temple of cyber-security



Key drivers for Security R&I

Usable security

- It is said that ‘The user is weakest link’, but often this means that security measures are badly designed or implemented.
- If security measures are difficult to use, people will make mistakes.
- If they conflict with productivity, pressures to by-pass them.
- Make people part of the solution:
  - Educate and motivate
  - User-centred design
  - People and computers have complementary strengths and weaknesses
  - Use human ability to compensate for machine weaknesses and vice versa

Co-operation and interoperability

- Vulnerabilities often appear at boundaries/interfaces
- Common approach and shared resources across departments
  - Secure Software/Systems Lifecycle
  - Open standards
  - Certification and qualification of vendors
  - Cybersecurity Operations Centre and Incident Response Team
  - Cybersecurity education and awareness
  - Penetration testing service
- Cooperation between public and private sectors and between nations
  - National CERT to co-ordinate sharing of cyber-security intelligence
- Address shortage of cyber-security skills

UK Government Security Policy Framework – Overarching Principles

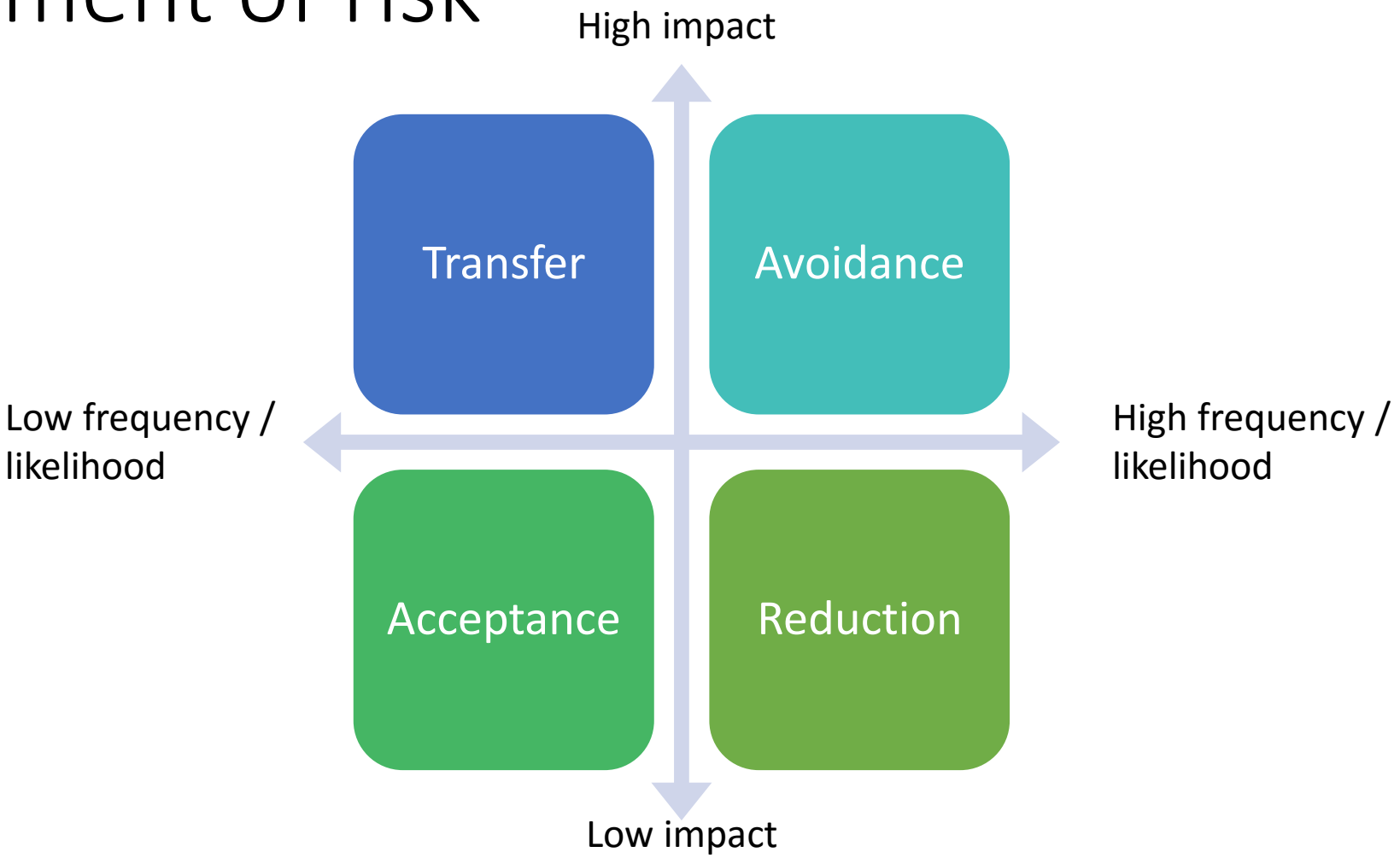
1. Protective security should reflect the UK's widest national security objectives and ensure that HMG's most sensitive assets are robustly protected.
2. Security must enable the business of government and should be framed to support HMG's objectives to work transparently and openly, and to deliver services efficiently and effectively, via digital services wherever appropriate.
3. Risk management is key and should be driven from Board level. Assessments will identify potential threats, vulnerabilities and appropriate controls to reduce the risks to people, information and infrastructure to an acceptable level. This process will take full account of relevant statutory obligations and protections, including the Data Protection Act, Freedom of Information Act, the Official Secrets Act, Equality Act and the Serious Organised Crime and Police Act.
4. People and behaviours are fundamental to good security. The right security culture, proper expectations and effective training are essential.
5. Policies and processes will be in place for reporting, managing and resolving any security incidents. Where systems have broken down or individuals have acted improperly, the appropriate action will be taken.

Recap of main points

- Digital technology offers many benefits, but also brings danger for the unwary
- Concerns about cyber-security are one of the main pacing factors governing the rate of digital innovation, including
  - Virtualisation and cloud computing
  - Big data and intelligent analytics
  - Internet of Things and Smart ‘X’
    - X = Cities/Health/Transport/Manufacturing/Transport …
- There are no secure systems!
  - Risk-led approach combining protection, detection, response and recovery
  - Recognise organisations as socio-technical systems – see people as part of the solution, not part of the problem
  - Co-operation and intelligence sharing

Reserves

Treatment of risk



Types of cyber-threat agent