Lebanon Digital Transformation

التحـــول الرقمـــي في لبنـــان

DIGITAL TRANSFORMATION CONFERENCE 2018

مـؤتمـر التحـول الـرقمـي 2018

Republic of Lebanon

OMSAR

Office of the Minister of State for Administrative Reform

SUPPORTED BY:

WORLD BANK GROUP

Cybersecurity at Scale: Securing Government Digital Services

Paul Kearney

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
  - 20 years at British Telecom, Adastral Park, Martlesham Heath, Ipswich. Most recently as Chief Researcher in the Security Futures Practice, Research and Innovation.
  - Currently:
    - Professor of Cybersecurity at BCU (50%)
    - Visiting Scholar at EBTIC, Khalifa University, Abu Dhabi (25%)
    - Exploring other opportunities and interests (25%)

What CIOs and CISOs are saying about DT and cybersecurity (from Forbes survey):

- 69% of senior executives say digital transformation is forcing fundamental changes to security strategies
- 64% will boost spending to protect against known security threats
- 43% will make timely patching and remediation a higher priority in 2017
- 68% plan to enhance incident response capabilities in the next 12 months
- Operations teams are seeing heightened accountability for security breaches
- 72% believe line-of-business managers must take a greater role in developing security strategies
- Nearly half of enterprises will combine security and operations personnel into teams for fortifying mission-critical applications

'Enterprises re-engineer security in the age of digital transformation', Forbes Insight report, Jan 2017

Recommendations of Forbes report

1. Create a modern cybersecurity strategy backed by a solid business model
2. Redouble efforts to secure mission-critical assets
3. Improve organizational effectiveness by investigating new reporting structures
4. Develop an enterprise-wide culture of security.
5. Shift thinking from safeguarding applications to securing the data itself

What can go wrong?

US Office of Personnel Management (OPM) data breach:

- In June 2015, OPM discovered that the background investigation records of current, former, and prospective Federal employees and contractors had been stolen. 21.5 million individuals were affected.
- Earlier in 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been stolen.
- State-sponsored Chinese hackers rumoured to be responsible

The human factor in securing digital services

- Digital services provided by a combination of People, Processes and Technology.
- Educate staff so that they become a security asset rather than a liability
- Design processes and technology to facilitate secure behaviour and avoid potential for mistakes
- Incentivise secure behaviour and avoid conflicts of interest, e.g. between productivity and security

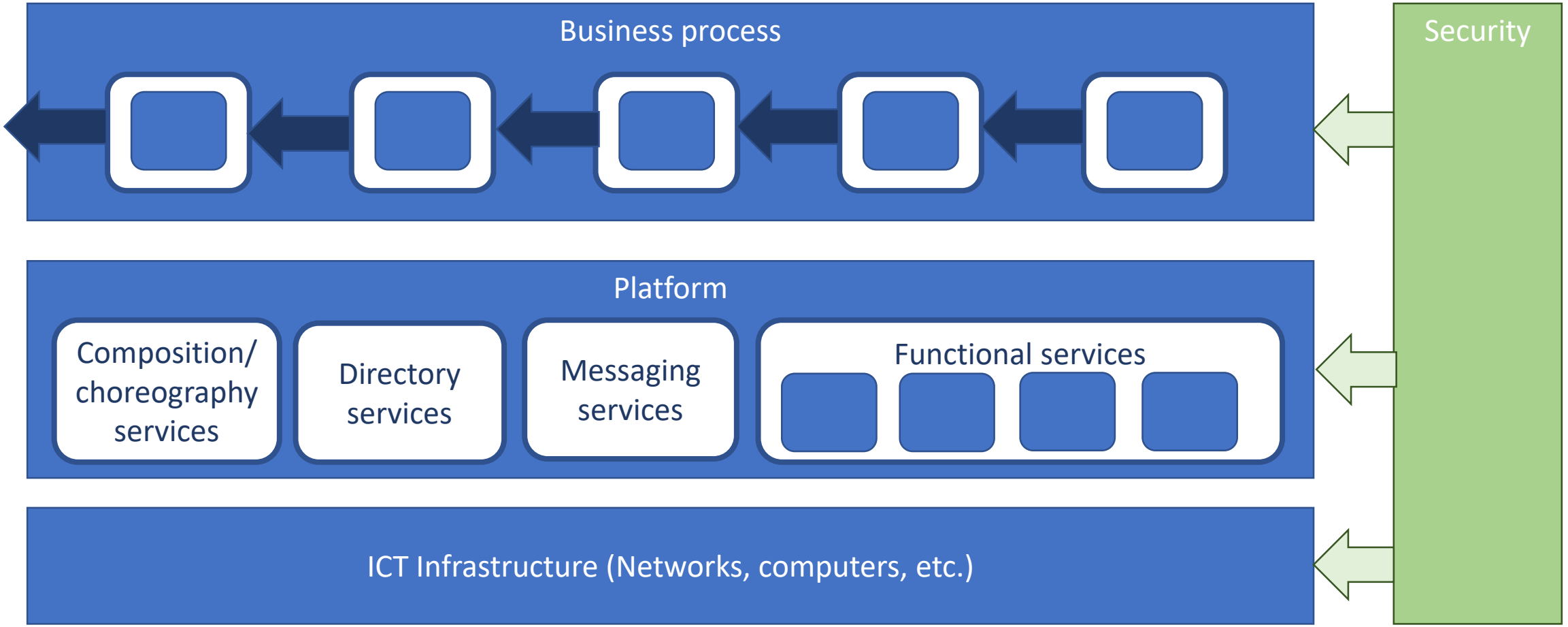
Security principles for digital services

1. Only provide service to authorised beneficiaries. (Analogous to Confidentiality)
2. Ensure process providing service is enacted correctly. Prevent attackers from modifying process or associated software and data. (Service Integrity)
3. Service should always be available to legitimate beneficiaries. Attackers must not be allowed to prevent delivery of service. (Service availability)
4. Enactment of process providing service should not acquire or reveal information about the beneficiary unnecessarily. (Privacy)
5. Evidence of service transaction should be available to beneficiary and provider. (Accountability / Non-repudiation)

Complementary ways to implement security

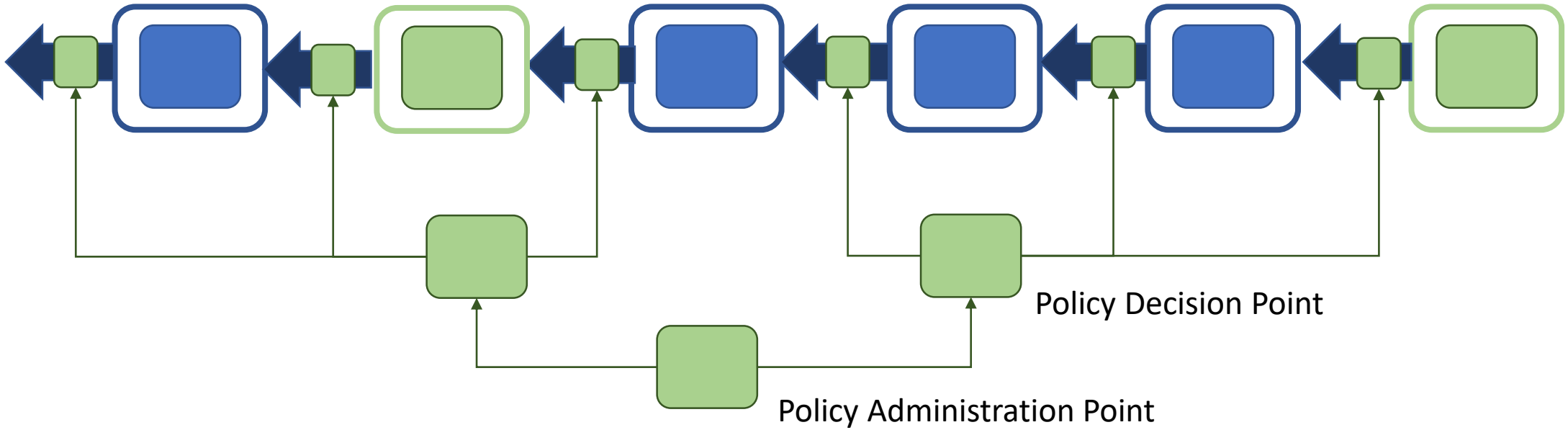
1. Hardening / security by design:
   - Avoid / remove potential vulnerabilities and unnecessary functionality and complexity.
   - KISS = keep it simple and secure
2. Enforcement and protection
   - Additional functionality to enact security policies and prevent attacks succeeding
3. Detect, respond and recover
   - Actively look for evidence of active attacks and successful breaches and respond appropriately

Service-oriented architecture



Service-oriented security

Business process + security policies -> secure business process



Conclusions

- Government digital transformation requires a new approach to cybersecurity focused on protection of digital assets and the ability to provide services to citizens. It must:
  - Recognise that digitally-transformed organisations are socio-technical systems
  - Address security within Business Process, Platform and Infrastructure layers, and holistically. Harden, protect, enforce policies, detect, respond and recover.
- Service-oriented architecture needs service-oriented security
  - Compose business process with security policy to obtain a secure business process

THANK YOU
شكراً