Top Challenges and Solutions for SMEs

Simon Parkin
University College London
Background

- Human factors of security research
  - Security usability, policy comprehension and awareness

- Work with large organisations (~10Ks of staff)
- … and small ones (1-50 members)
  - Small-to-Medium Enterprises (SMEs)
  - Small charities

- Collaborating with
  - Imperial College, to model security investment and the *indirect (human) costs* of security
  - Outsourced IT providers, to understand security challenges SMEs face in practice
Indirect cost example: ‘wall of disruption’
SMEs security challenges

- Formal security training and in-house expertise is … … limited … or non-existent
- Security policies and guidelines a challenge to interpret
  - Despite good intentions

- Leased services, and controls intended for home users
  - Little control or oversight
  - Resourcing challenges

- Employees need to learn and adapt IT
- Where technology design ignores staff needs, resistance can happen
Compliance Budget

Organisational effort required for compliance

Individual effort expended on compliance

Compliance Threshold
SMEs are diverse
Solutions - initial insights

1. Focus training on core threats to the business
   - Example: phishing training to limit credential theft
   - SMEs operate with less infrastructure and resources

2. Checklists are one way to overcome technical jargon
   - Situate advice, and avoid tech-speak which reads like it is “for someone else”

3. Weave security training into other procedures
   - Security is just one hat that people wear
References