Beyond the Office Walls: Understanding Security and Shadow Security Behaviours in a Remote Work Context

Sarah Alromaih[1] Ivan Flechais[1] George Chalhoub[1,2]

University of Oxford[1]
University College London[2]

Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)

Introduction

- Remote work experienced a boom post-pandemic, contrasting with the steady increase observed between 1980 and 2019
- According to 2022 workplace trends and insights report:
  - 73% of employees in hybrid or fully remote settings
  - Nearly half work entirely from home
  - One third prefer to continue working fully remote
- Remote work includes various modalities:
  - Location: home, communal spaces (libraries, coffee shops), or co-working environments
  - Flexibility: asynchronous work or hybrid model

Motivation

- Organisational security research has primarily focused on user security behaviour ***within*** workplace boundaries, categorising it as *compliant*, *non-compliant*, or *shadow security behaviours*
- Shadow security behaviours refer to practices developed by security-conscious users when they are unable to follow official security policies
- Despite growing research in remote work:
  - There has been insufficient exploration of how workers interact with organisational security policies in remote settings
  - Existing studies of remote work have not focused on user security behaviour, particularly shadow security, which has only been examined within organizational contexts

Methodology

- **Research Question:** What are the current security and shadow security practices in remote work?

- **Approach:** Constructivist Grounded Theory to collect and analyse data

- **Study:** Iterative process of interview and analysis with 20 remote workers
  - employed by external organisations
  - 9 hybrid and 11 fully remote

Results

Our analysis identified 217 codes which we organized under the following themes:

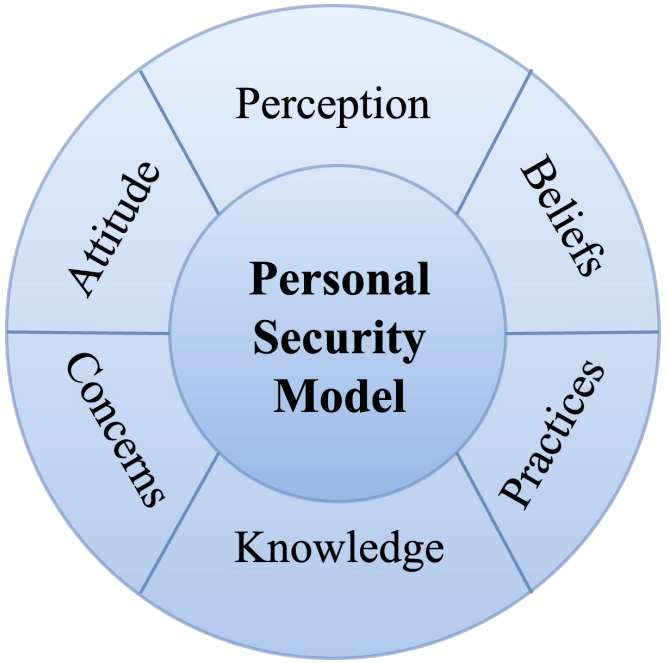
- Personal Security Model
- External Security Influences
- Organisational Security Model
- Personal-Organisational Security Appraisal in Remote Work

Personal Security Model

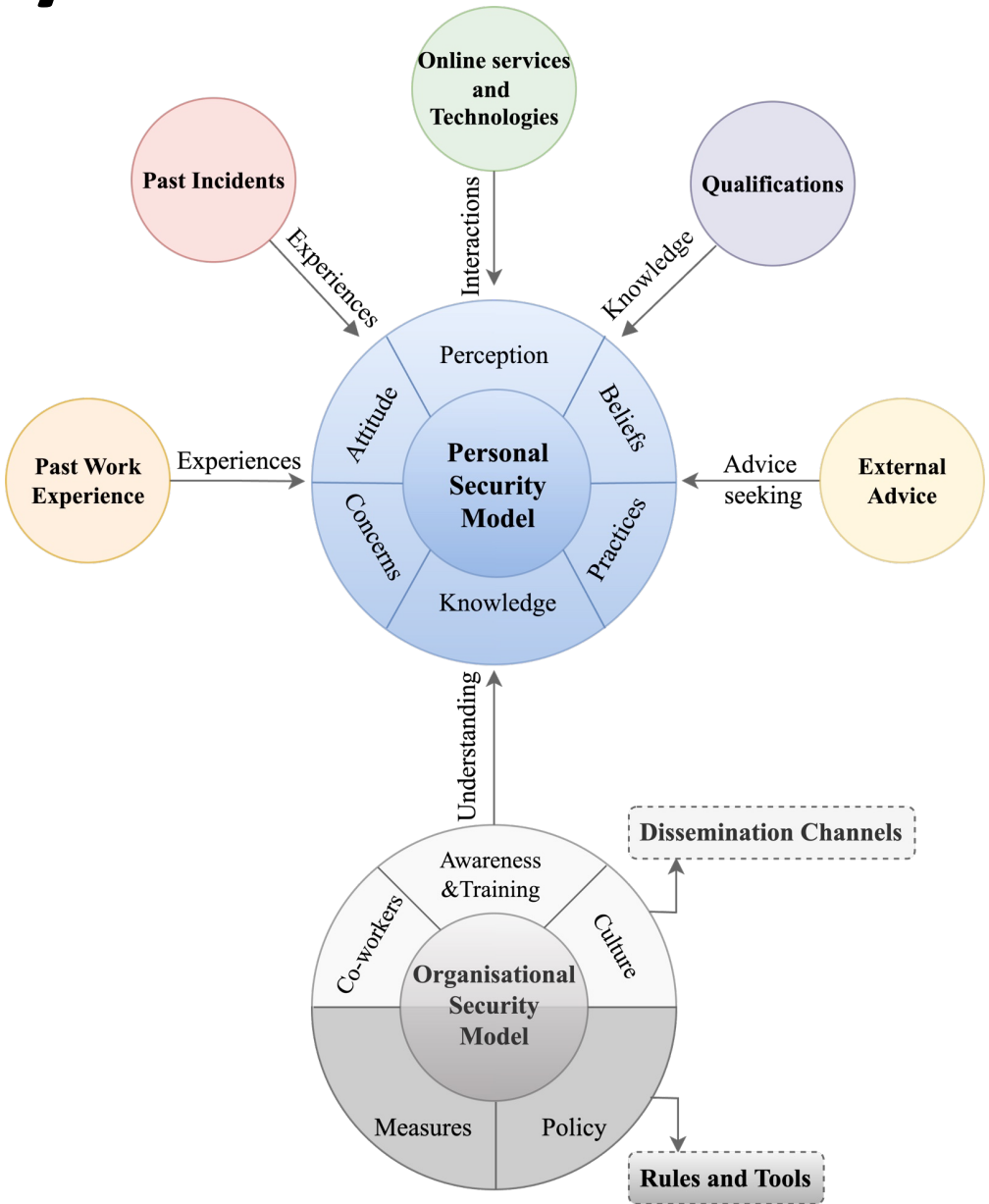
- Composed of individual attitude, perception, knowledge, concerns, beliefs and practices for personal security

- Guides personal behaviour for all security: including home and remote work security

- Shaped by individual experiences and interactions with the environment

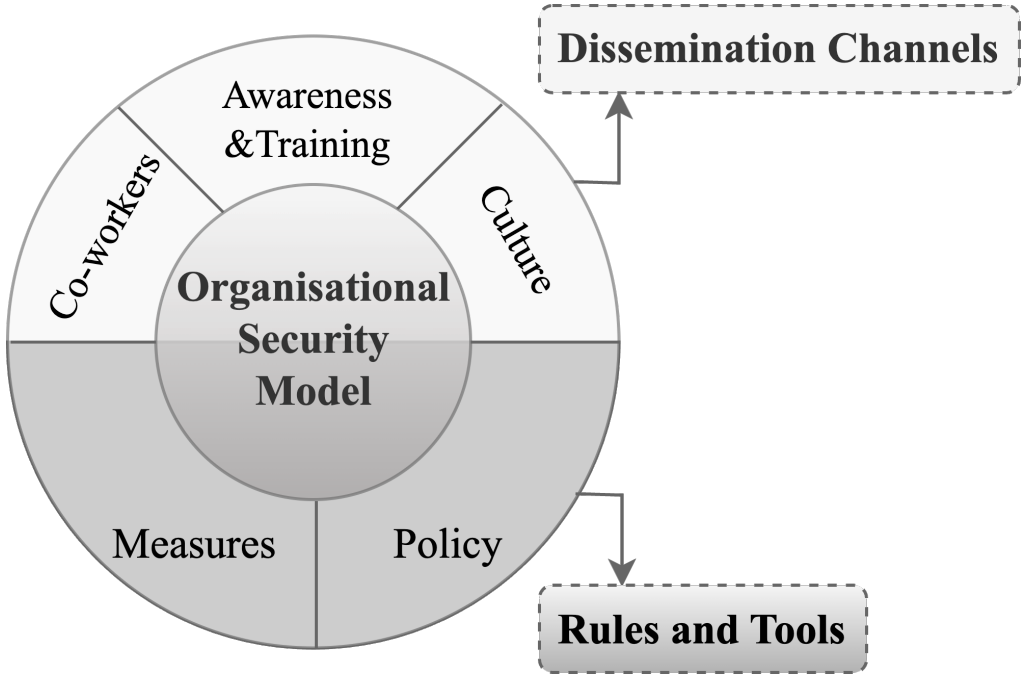


External Security Influences

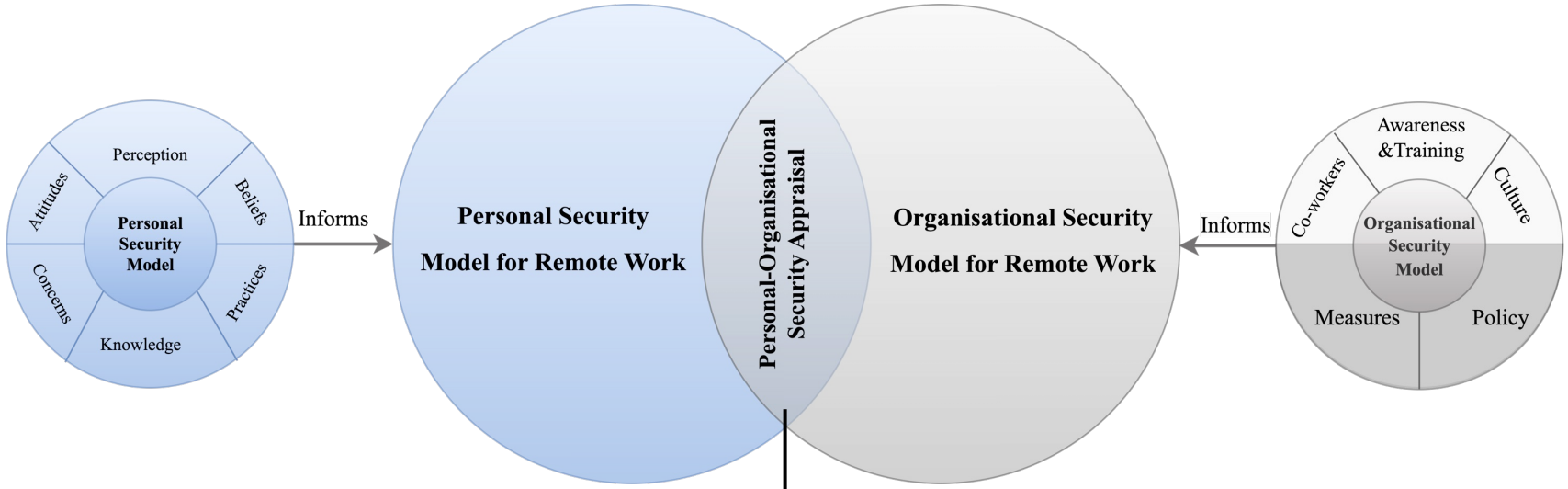


Organisational Security Model

- **Rules and Tools:**
  - **Rules:** security policies specifying what individuals should and should not do
  - **Tools:** technical means to enforce rules (e.g., VPN, endpoint management, MFA)
- **Dissemination Channels:**
  - **Direct**: security awareness and training programs
  - **Indirect**: security culture and co-worker interactions



Personal-Organisational Security Appraisal in Remote Work

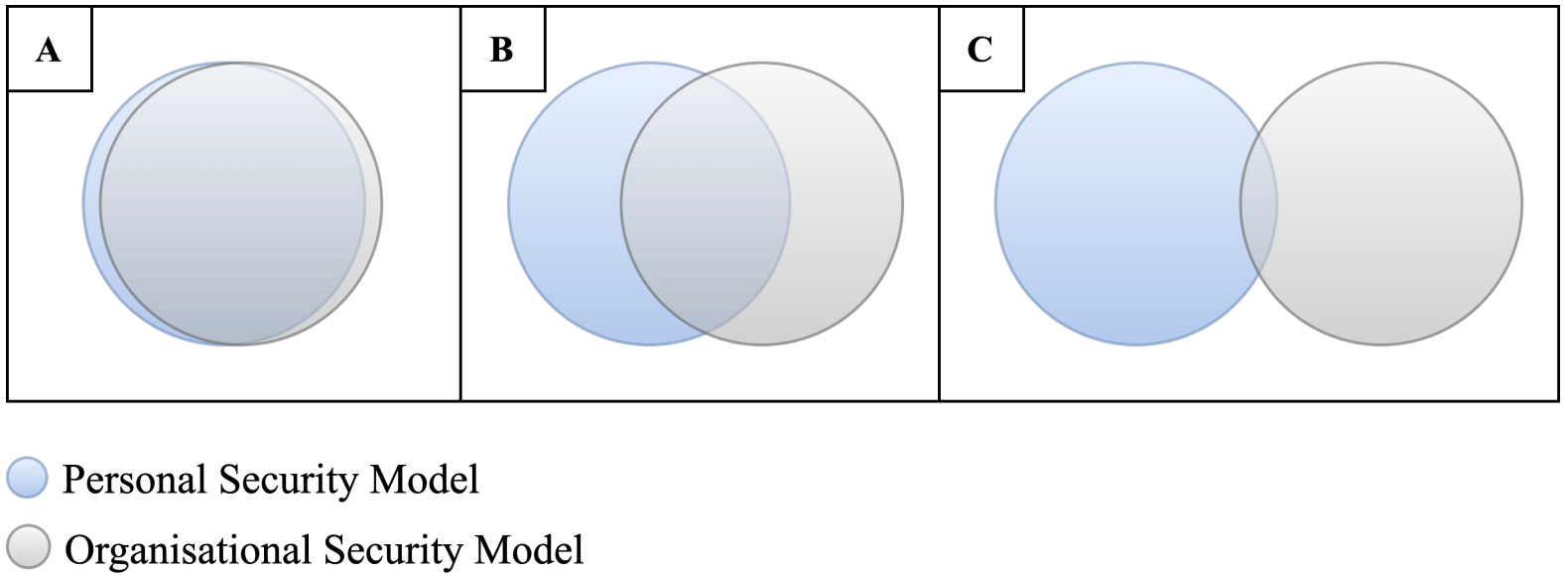


Influence user security-related behaviour in remote work

Not grounded in objective truth but in user perception.

Explains compliance, noncompliance, and shadow security behaviour.

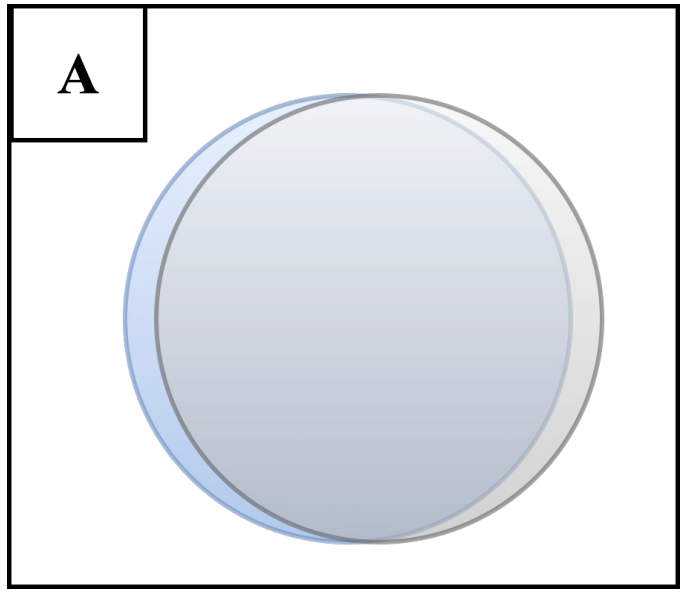
Types of Alignment



A. Security Models are Well Aligned

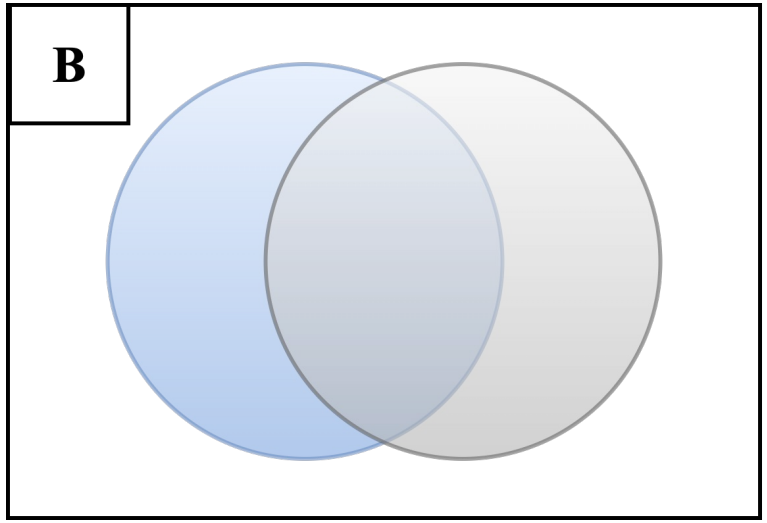
- Users experience no problems with the provision of remote work facilities

- Participants reported compliant security behaviours
  - e.g., using organization-provided devices



B. Security Models are Partially Aligned

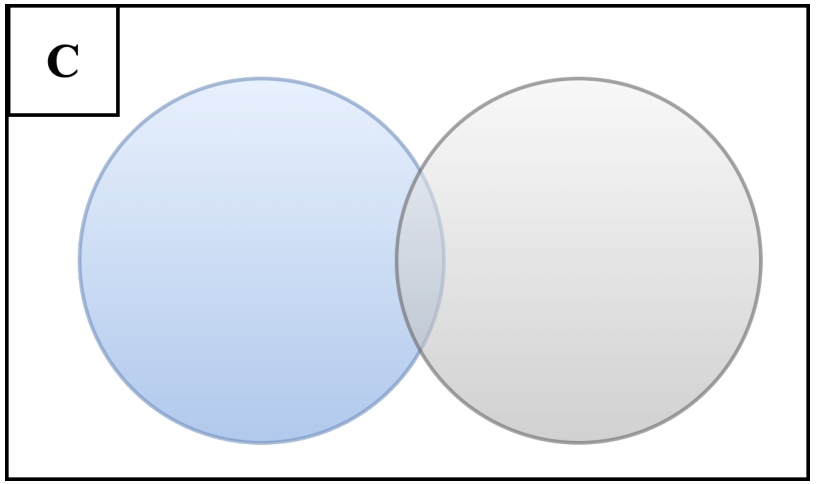
- Poorly compliant security behaviours
  - e.g., sporadic VPN usage, password reuse
- Proactive security behaviours in the absence of policy (*Shadow Security*)
  - e.g., enhancing home WiFi security
- Non-compliant security behaviours driven by security (*Shadow Security*)
  - e.g., using Secure Dropbox instead of the provided cloud service



C. Security Models are Poorly Aligned

- Participants reported instances of non-compliant behaviours
  - e.g., connecting to public WiFi without VPN; replacing hard drive on work device; using insecure file sharing service

- **Justifications:** convenience; productivity; privacy concerns; slow IT response; underestimating security threats posed by workarounds



Discussion

- Shadow security practices adapt as organizational boundaries become less tangible and more flexible.

- Personal-organizational security appraisal process and the types of alignment:
  - explain how individuals relate their personal security perspectives to the organizational security model
  - offer valuable insights into explaining user security-related behaviour in remote work context
  - help diagnose and address the root causes of challenges in security practices

Discussion

- **Security Policy Limitations:** Shadow security behaviours address, extend and remediate perceived limitations of existing remote work policies
- **Usability Issues:** Complex security controls and lack of support lead to shadow security practices and usability concerns
- **Security Awareness and Training:** Effective security training benefits both current and future employers, especially in the gig economy
- **Security Communications:** Security knowledge is disseminated in many ways (awareness training, colleagues, and broader security culture), however many of these forms of communication are absent or limited in remote work

Future Research Opportunities

- Facilitating informal security communication in remote settings
- Homogenising security interactions
- Adopting user experience design for remote work solutions
- Exploring security awareness and training for remote work

Thank you

Any questions, please contact:

sarah.alromaih@cs.ox.ac.uk