NEXIS

# Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Access

SOUPS‘24, Philadelphia, USA – Aug 12, 2024

Thomas Baumer, Tobias Reittinger, Sascha Kern, Günther Pernul

# Who we are

### Thomas Baumer

- PhD Student
- Software Engineer

- Access Control
- Maintenance

NEXIS

### Tobias Reittinger

- PhD Student
- Research Assistant

- Cybersecurity Incentives
- Cybersecurity Motivation

UR
Universität Regensburg

### Sascha Kern

- PhD Student
- Software Engineer

- Access Control
- Data Quality

NEXIS

### Günther Pernul

- Fulltime Professor
- Supervisor

- Cybersecurity
- Information Systems

UR
Universität Regensburg

# Agenda

1 Understanding the Problem

2 Asking Experts for Advice

3 Choice Defaults User Study

4 My Takeaways and Request

# Access Reviews: The Problem and its Challenges

An understudied usable security problem

### Formalization of the Problem

**(Our work, SOUPS, 2024)**

| | | Authorization | |
|---|---|---|---|
| | | Positive *PP* | Negative *PN* |
| **Security Policy** | Positive *P* | *TP* | *FN* |
| | Negative *N* | *FP* | *TN* |

**Primary Goal:** Reduce Excessive Authorizations (FP)

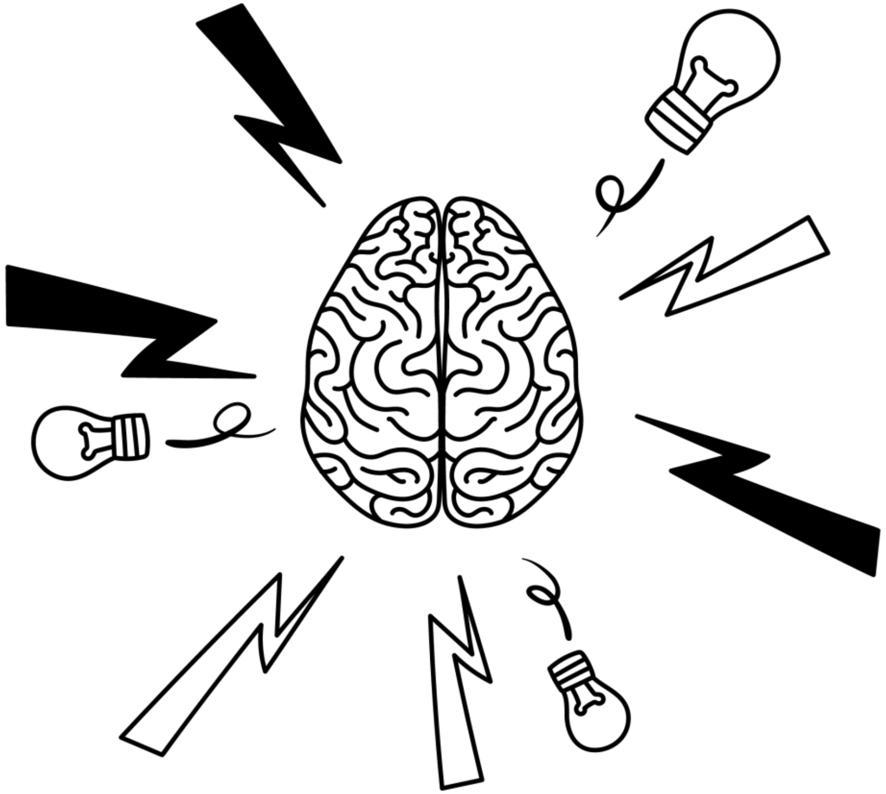
(Experts' estimation for *FP*: *M*=22.8%, *SD*=6.4%, *n*=10)

### Expert Interviews on Access Review Challenges

**(Jaferian et al., SOUPS, 2014)**

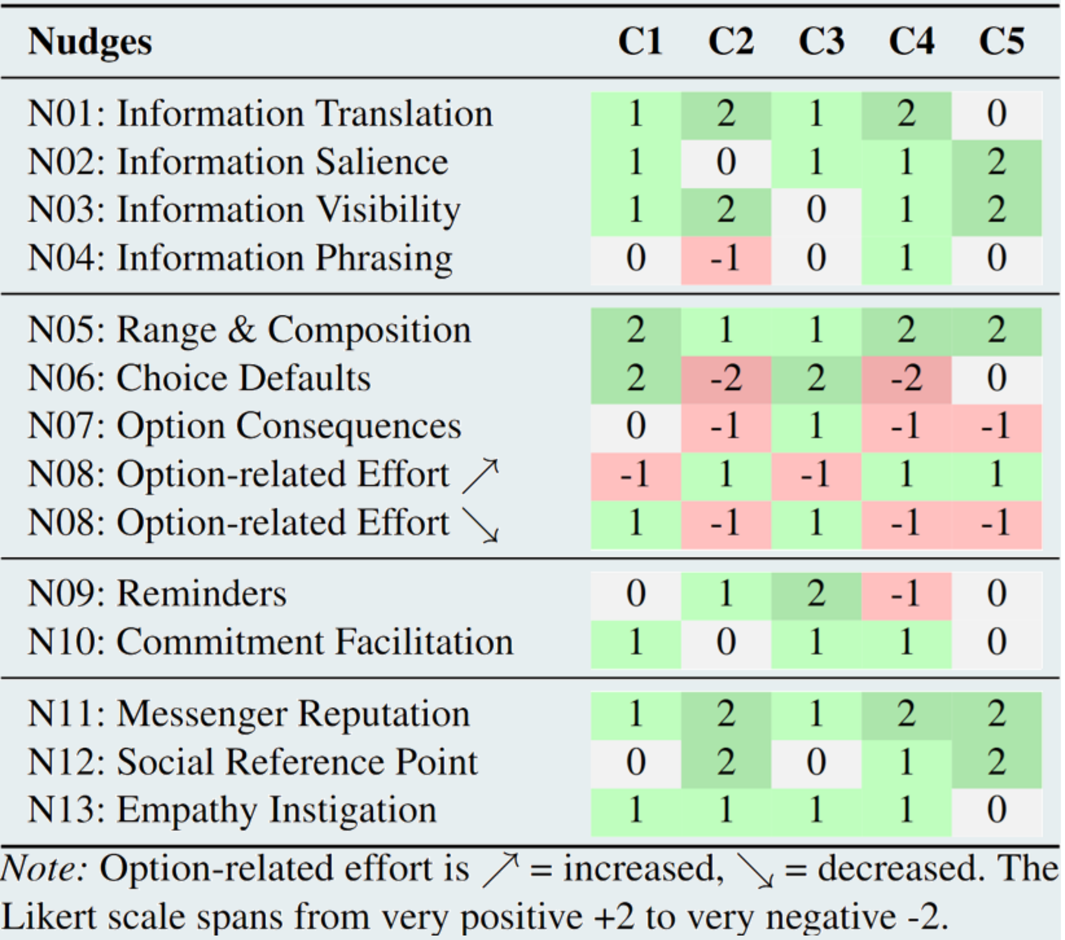
1. Scale
2. Lack of Knowledge
3. Frequency
4. Human Errors
5. Exceptional Cases

# Asking Experts for Advice



# Can Digital Nudges help?

Access Review Experts on the Application of Digital Nudges.



| Nudges | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|
| N01: Information Translation | 1 | 2 | 1 | 2 | 0 |
| N02: Information Salience | 1 | 0 | 1 | 1 | 2 |
| N03: Information Visibility | 1 | 2 | 0 | 1 | 2 |
| N04: Information Phrasing | 0 | -1 | 0 | 1 | 0 |
| N05: Range & Composition | 2 | 1 | 1 | 2 | 2 |
| N06: Choice Defaults | 2 | -2 | 2 | -2 | 0 |
| N07: Option Consequences | 0 | -1 | 1 | -1 | -1 |
| N08: Option-related Effort ↗ | -1 | 1 | -1 | 1 | 1 |
| N08: Option-related Effort ↘ | 1 | -1 | 1 | -1 | -1 |
| N09: Reminders | 0 | 1 | 2 | -1 | 0 |
| N10: Commitment Facilitation | 1 | 0 | 1 | 1 | 0 |
| N11: Messenger Reputation | 1 | 2 | 1 | 2 | 2 |
| N12: Social Reference Point | 0 | 2 | 0 | 1 | 2 |
| N13: Empathy Instigation | 1 | 1 | 1 | 1 | 0 |

*Note:* Option-related effort is ↗ = increased, ↘ = decreased. The Likert scale spans from very positive +2 to very negative -2.

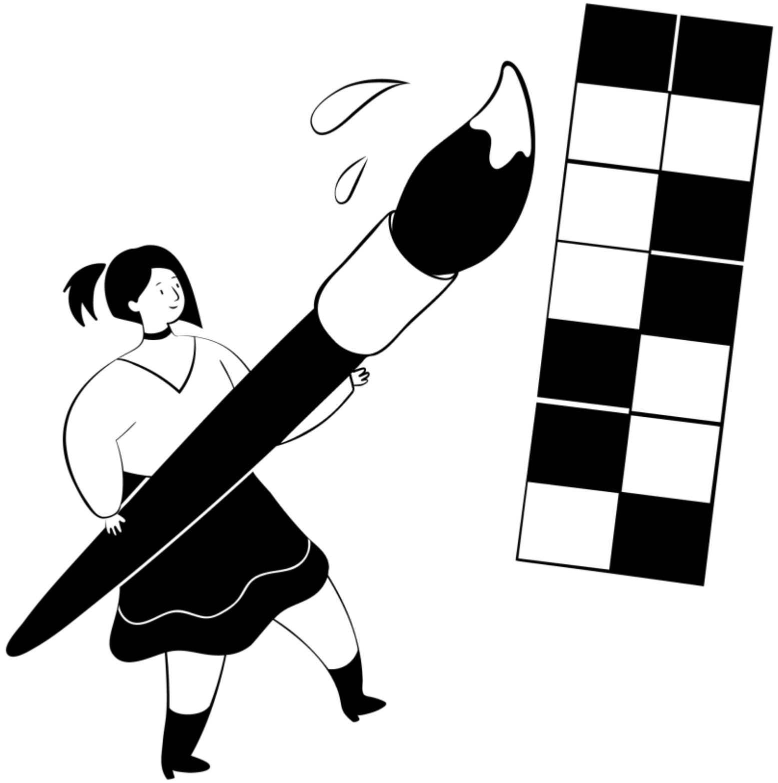
**Method:**

- 10 expert interviews with mean duration ca. 60 minutes
- Building upon present literature

**Takeaways:**

- Most nudges are promising and worth a dedicated study.
- Careful consideration is necessary.

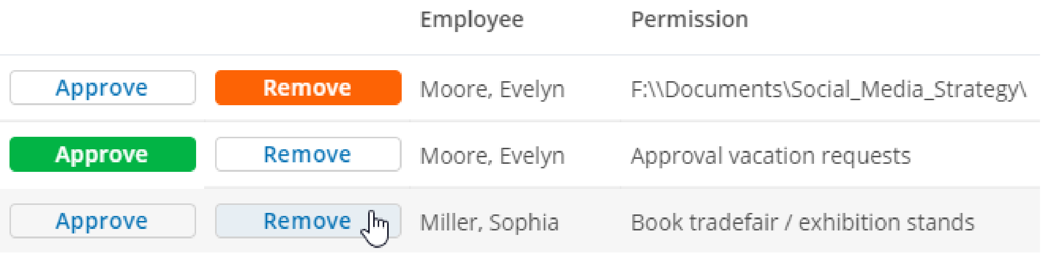
# Choice Defaults User Study



# Let‘s study the Choice Defaults Nudge!

## Method

- Three groups: default accept, default reject, and neutral
- 102 participants (34 for each group)
- Reviewing 160 authorizations based on case study
- Observation
  - Decisions and time consumption
  - Accuracy and errors
  - Self-assessment with NASA TLX

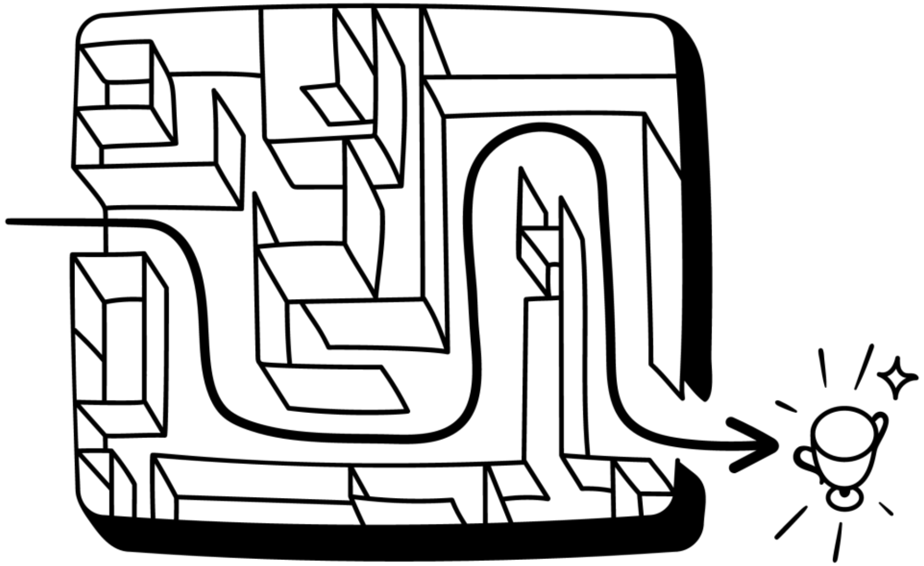


| | | Employee | Permission |
|---|---|---|---|
| Approve | Remove | Moore, Evelyn | F:\\Documents\Social_Media_Strategy\ |
| Approve | Remove | Moore, Evelyn | Approval vacation requests |
| Approve | Remove | Miller, Sophia | Book tradefair / exhibition stands |

## Takeaways

- Influence on decisions
  - Default reject -> more revokes
  - Deciders did not blindly follow the nudge
- Deciders’ perception
  - Reduced stress perception
  - Reasonable performance perception
- Objective measurements
  - Time saves
  - Quality improvement **not** out-of-the-box

# My Takeaways and Request



# My General Takeaways

- Ignoring human factors in access reviews is a bad idea (imho).
- Divide and conquer: Ask questions in context!
- My request: **Study access reviews!**
  - An understudied usability problem for security.
  - We worked on foundations, but advances are feasible!
  - Availability: https://github.com/AccessReview/Availability

# Contact me

Thomas Baumer

Software Engineer, PhD Student

thomas.baumer@nexis-secure.com

+49 160 98280534