Discussion of
"The Persistence of Subjective Threat Perceptions and Public Compliance"
by
Richard J. Goodlin Sen. and Oliver Vaught
and
Cynthia Lin and Mark A. Murphy, Chair

Amanda Kass
Harvard Law School

Summary

Goodlin Sen. and Vaught argue that we can explain variation in the persistence of subjective threat perceptions after major events by looking at the role of social networks. I discuss their argument and suggest that it could be strengthened by (1) providing more information about the data and methods used to measure social networks, (2) considering alternative explanations for the persistence of subjective threat perceptions, and (3) discussing the implications of the findings for theories of risk perception and behavior.

Setting

Research on risk perception has a long history in psychology, sociology, and political science. Goodlin Sen. and Vaught's paper builds on this literature by focusing on the role of social networks in shaping individuals' perceptions of risk. They argue that social networks can help to explain why some people continue to perceive a high level of risk long after the immediate danger has passed, while others return to their pre-event level of risk perception relatively quickly.

Findings

Goodlin Sen. and Vaught's paper makes a number of important contributions to the literature on risk perception and behavior. The authors provide a clear and well-motivated theoretical framework for understanding the role of social networks in shaping individuals' perceptions of risk. They also present a novel and innovative empirical strategy for measuring the persistence of subjective threat perceptions. The paper's findings have important implications for both theory and practice.

Did he/she think of this?

1. Account Lock Name

Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.

- Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                        - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                          - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                            - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                              - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                                - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                                  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                                    - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
                                                                                                                                                                                                      - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed log-in attempts. Look out for the duration of the lockout policy. Too short a duration gives an attacker more time to brute force the account. Too long a duration paves the way for a denial-of-service attack on all users.
  - Lock the account after a number of failed

Discussion of "Tax Revenue Risk, Municipal Bond Yield, and Public Investments"

Da Huang, Vasudha Nair, and Nathan Seegert

FRB Chicago Conference on Municipal Bond Markets, 2026

Kenneth Ahern

USC University of Southern California

NBER National Bureau of Economic Research

Summary

Hypothesis: Municipal bond prices reflect systematic tax risk
If tax revenues are low in bad states, then higher yields

Method

Measure tax risk as covariance of sales, income, corp. tax with GDP
State level data from 2002-2023
Regressions on local-level bond yields on tax risk
Cross-border discontinuity test

Findings

Bond yields reflect tax risk
Robust to alternative explanations
Lowers public investment

First Hurdle: Should we care?

First Hurdle: Should we care?

Yes! Important question!

- Understanding municipal bond pricing is important
- Little work investigating a systematic risk component
- Even though markets are fragmented, there is still commonality

First Hurdle: Should we care?

Yes! Important question!

- Understanding municipal bond pricing is important
- Little work investigating a systematic risk component
- Even though markets are fragmented, there is still commonality

Comments

1. Relevant cash flows

2. State tax vs. local municipal bonds

3. Measurement of tax risk

4. Causal identification

1. Relevant cash flows

Systematic risk is covariance of cash flows with economic states
Which cash flows?

- This paper: tax revenues
    - Sales, personal income, corporate income taxes
- Why just these three?
    - Their fraction of total tax revenue varies across states
        - MA (84%) and CA (83%) vs. NH (29%) and VT (42%)
            - Average effect is controlled by state fixed effects
    - Vary within state over time
        - ND: 53% to 34% vs NH: 24% to 41%
            - State-year effect not controlled in the paper
            - This could drive tax risk

Different cash flows, different risk

Alternative 1: All tax revenue

Alternative 2: Tax revenues plus user fees

- User fees have become a larger component of local revenues
- Building permits, traffic tickets, utilities, licenses

Alternative 3: Taxes, fees, and intergovernmental transfers

- This possibly represents what bond holders care about
- Governmental transfers can work as insurance
  (Gao, Lee, and Murphy, 2019, JFE)

At the least, these alternatives should be in robustness

2. State tax vs. municipal bonds

The paper's empirical outcome is municipal-level bond yields

- Cities, counties, school boards, development districts

The paper's key explanatory variable is state-level tax risk

This is problematic conceptually and statistically

- It is not obvious that state-tax risk is an appropriate proxy
    - Local governments collect different types of taxes
        State of Texas: No property tax at state level
        Houston: 49% property tax
- Statistically
    - Much less true variation than it seems by large N

Should calculate local level tax risk or run analysis for state bonds

3. Measurement of tax risk

The key explanatory variable is tax risk

Starts with value of a revenue tax stream (R) with state price m:

$$E[m_t R_t] = \underbrace{E[m_t]\,E[R_t]}_{\text{certainty equivalent}} - \underbrace{\big(-\operatorname{Cov}(m_t, R_t)\big)}_{\text{tax risk}}$$

Tax risk calculated over lagged 4 observations:

$$\text{Tax Risk}_{s,t} = \frac{-\operatorname{Cov}(\pi_{s,t},\, R_{s,t})}{E[\pi_{s,t}\, R_{s,t}]}, \qquad \pi_{s,t} = \frac{1}{1+g_{s,t}}$$

g: state GDP growth; pi is reciprocal of gross growth
Denominator scales out state size

Empirical calculation does not match the theoretical equation

Data on state GDP and tax revenues are straightforward
I can replicate the summary stats of tax and GDP variables
Ensures I have the right states, years, GDP measure, tax accounts

	My replication					Paper, Table 1				
	Mean	SD	p10	p50	p90	Mean	SD	p10	p50	p90
Tax Volatility^{sd}	0.07	0.05	0.02	0.06	0.13	0.07	0.05	0.02	0.06	0.13
Tax Volatility^{g}	0.07	0.04	0.04	0.07	0.12	0.07	0.04	0.04	0.07	0.12
Tax Revenue / GDP (%)	5.39	1.25	3.93	5.24	7.01	5.39	1.25	3.93	5.24	7.01
GDP Growth (%)	4.49	3.79	0.51	4.22	9.12	4.39	3.49	0.10	4.30	8.50

Empirical calculation does not match the theoretical equation

Data on state GDP and tax revenues are straightforward
I can replicate the summary stats of tax and GDP variables
Ensures I have the right states, years, GDP measure, tax accounts

	My replication					Paper, Table 1				
	Mean	SD	p10	p50	p90	Mean	SD	p10	p50	p90
Tax Volatility^{sd}	0.07	0.05	0.02	0.06	0.13	0.07	0.05	0.02	0.06	0.13
Tax Volatility^{g}	0.07	0.04	0.04	0.07	0.12	0.07	0.04	0.04	0.07	0.12
Tax Revenue / GDP (%)	5.39	1.25	3.93	5.24	7.01	5.39	1.25	3.93	5.24	7.01
GDP Growth (%)	4.49	3.79	0.51	4.22	9.12	4.39	3.49	0.10	4.30	8.50
Tax Risk (Eq. 2)	**0.0004**	**0.0020**	**−0.0010**	**0.0001**	**0.0028**	**0.04**	**0.02**	**0.02**	**0.04**	**0.06**

Empirical calculation does not match the theoretical equation

Data on state GDP and tax revenues are straightforward
I can replicate the summary stats of tax and GDP variables
Ensures I have the right states, years, GDP measure, tax accounts

	My replication					Paper, Table 1				
	Mean	SD	p10	p50	p90	Mean	SD	p10	p50	p90
Tax Volatility^{sd}	0.07	0.05	0.02	0.06	0.13	0.07	0.05	0.02	0.06	0.13
Tax Volatility^{g}	0.07	0.04	0.04	0.07	0.12	0.07	0.04	0.04	0.07	0.12
Tax Revenue / GDP (%)	5.39	1.25	3.93	5.24	7.01	5.39	1.25	3.93	5.24	7.01
GDP Growth (%)	4.49	3.79	0.51	4.22	9.12	4.39	3.49	0.10	4.30	8.50
Tax Risk (Eq. 2)	**0.0004**	**0.0020**	**−0.0010**	**0.0001**	**0.0028**	**0.04**	**0.02**	**0.02**	**0.04**	**0.06**

The tax risk variable does not replicate using the same data

Empirical calculation does not match the theoretical equation

Data on state GDP and tax revenues are straightforward
I can replicate the summary stats of tax and GDP variables
Ensures I have the right states, years, GDP measure, tax accounts

	My replication					Paper, Table 1				
	Mean	SD	p10	p50	p90	Mean	SD	p10	p50	p90
Tax Volatility^{sd}	0.07	0.05	0.02	0.06	0.13	0.07	0.05	0.02	0.06	0.13
Tax Volatility^{g}	0.07	0.04	0.04	0.07	0.12	0.07	0.04	0.04	0.07	0.12
Tax Revenue / GDP (%)	5.39	1.25	3.93	5.24	7.01	5.39	1.25	3.93	5.24	7.01
GDP Growth (%)	4.49	3.79	0.51	4.22	9.12	4.39	3.49	0.10	4.30	8.50
Tax Risk (Eq. 2)	**0.0004**	**0.0020**	**−0.0010**	**0.0001**	**0.0028**	**0.04**	**0.02**	**0.02**	**0.04**	**0.06**

The tax risk variable does not replicate using the same data

The paper's tax risk is 100x as large as the real calculation
The real calculation of tax risk is negative in 45% of state-years

A potential coding error replicates their results

If we replace the certainty equivalent $E[\pi]E[R]$ by $E[R]$:

$$TR^{CE}_{s,t} = \frac{E[R] - E[\pi R]}{E[\pi R]}$$

then, we can replicate the variable used in the tables

Tax Risk	Mean	SD	p10	p50	p90
Paper, Table 1	0.04	0.02	0.02	0.04	0.06
TR^{CE}	**0.043**	**0.021**	**0.019**	**0.041**	0.068

The variables match the negative of this value:

- Rankings: MI highest, UT lowest; CT, MS, NJ top; WA, TX bottom
- Table 2: correlation with Volatility matches
- Table 3 values match

What this altered tax risk variable actually is

$$TR^{CE}_{s,t} = \frac{E[R] - E[\pi R]}{E[\pi R]} = \underbrace{\frac{(1 - E[\pi])\, E[R]}{E[\pi R]}}_{\approx \text{ avg. GDP growth}} + \underbrace{\frac{-\operatorname{Cov}(\pi, R)}{E[\pi R]}}_{\text{Eq. 2: tax risk}}$$

Average gdp growth is about 0.04, covariance term is about 0.0004
Growth term accounts for 97% of variance
Corr(TR, 4-year average GDP growth) = 0.993

The measure of tax risk is basically trailing state GDP growth

Which variable used in main regression tests?

- If incorrect version, then yields reflect past gdp growth
- If correct version, then magnitudes are very different
    - The s.d. of correct version implies implausibly large effects

4. Causal identification

To infer causality requires exogenous variation in tax risk

Paper uses a border design

- Compare neighboring counties across state lines
- Similar local economic conditions

This doesn't solve the endogeneity problem

- First, the paper uses state-level tax risk, not local level
- Second, even if the local economic conditions are similar, the state-level institutions differ
    - Tax rules, transfers, pensions, state oversight, etc.
    - Some state-level aspect affects bond yields
        - But it is not necessarily tax risk

Requires exogenous change in local tax risk that does not also affect other variables that could influence bond yields

Summary

Very well motivated paper

- Important and understudied research question
- Logical and coherent economic logic to hypothesis

Suggestions for improvement

- Broaden definition of fiscal cash flow and use local data
- Resolve the tax risk calculation
- Try to find an IV or natural experiment that provides exogenous variation in tax risk exposure

Thanks!