RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HUM-F03

“THE SYSTEM...IS PEOPLE!”: DESIGNING EFFECTIVE SECURITY UX

Zoe Lindsey

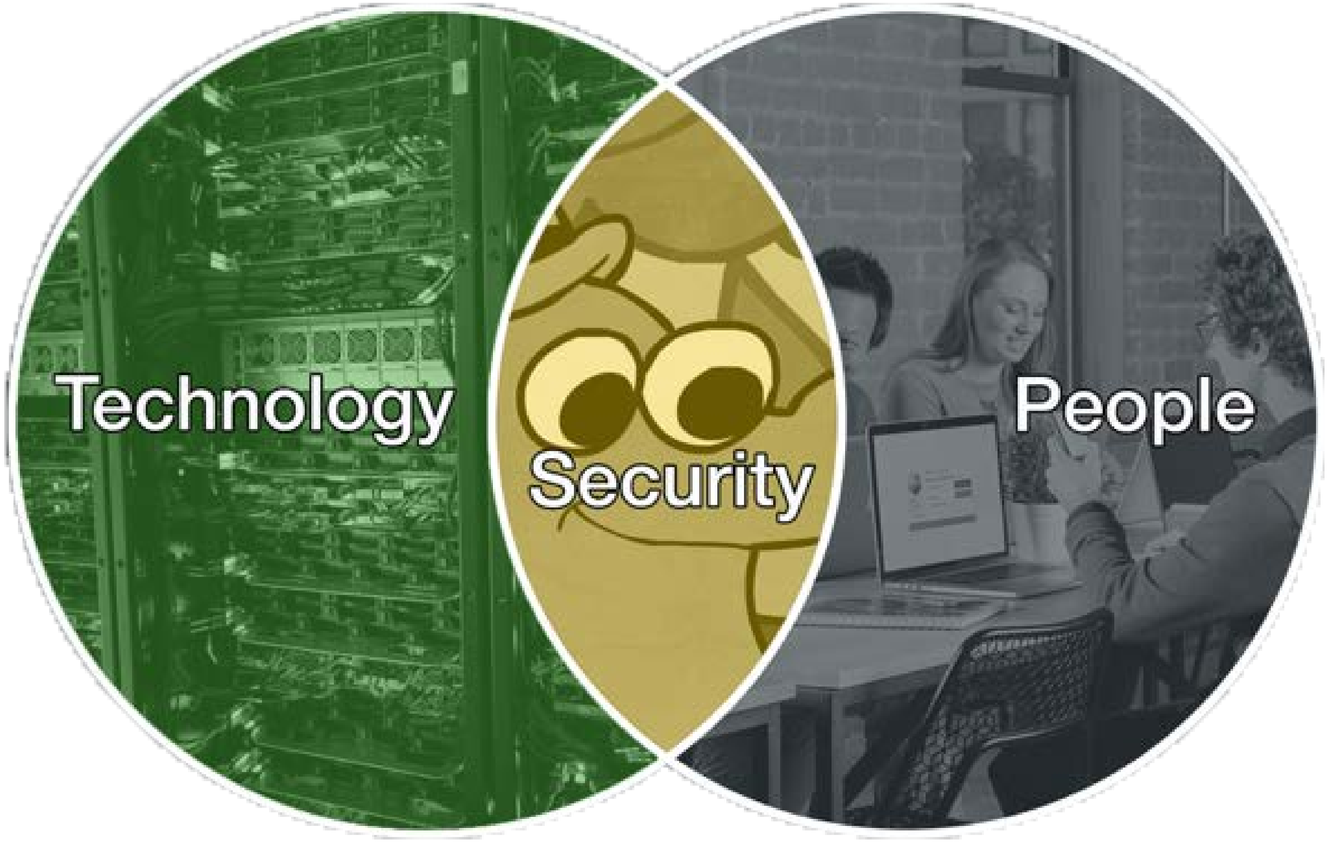
Advocacy Manager
Duo Security
@duozoe

The Space Between Risk and Reward

Does your organization have stated core values?

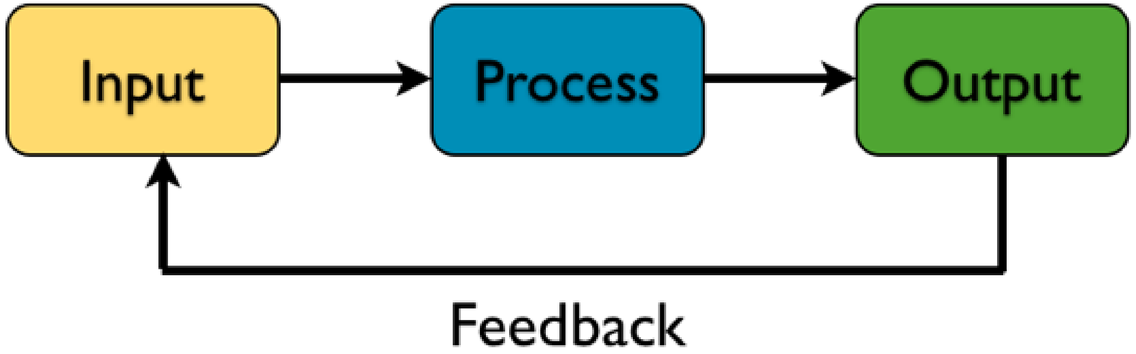
…is security one of them?

Our Security Strategy Is Lopsided



Security: the need exists at the intersection of technology and people

The Overlooked Critical System: Culture



PRIMARY INPUTS

- Shared norms, values, routines
- What the business rewards/punishes

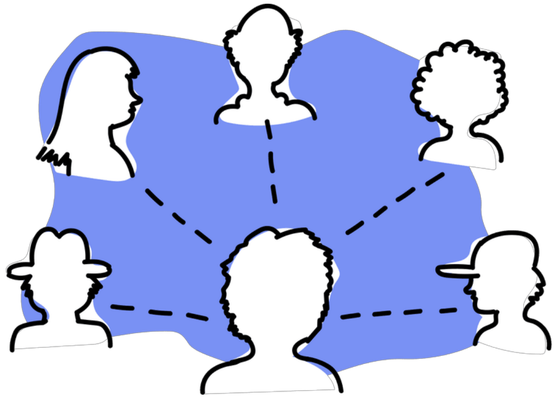
PRIMARY OUTPUTS

- User behavior
- Employee churn
- Organizational health

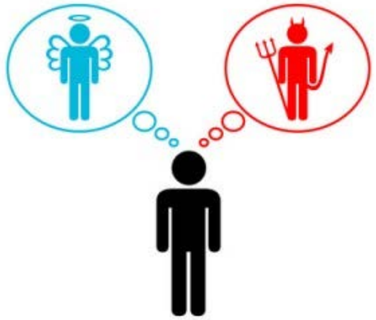
WHAT DETERMINES CULTURE?
(ENVIRONMENTAL VARIABLES)

Cultural Currency: What's My Motivation?

Economic



Social

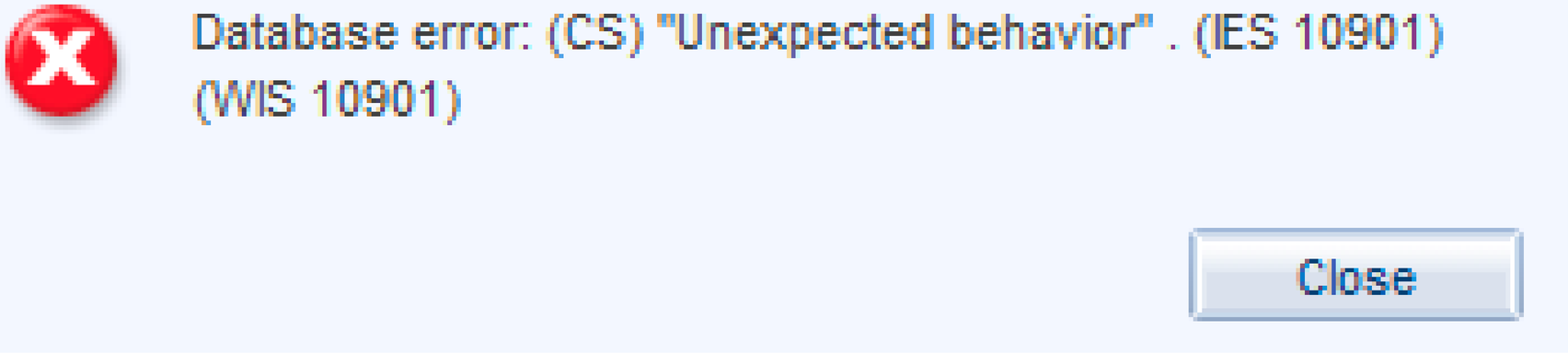


Moral

Crafting Conscientious Culture

Taiichi Ohno, Creator of the Toyota Production System (“Stop the Line”)

Unexpected Behavior, or Unacknowledged Incentive?



Example: Deadline Drama

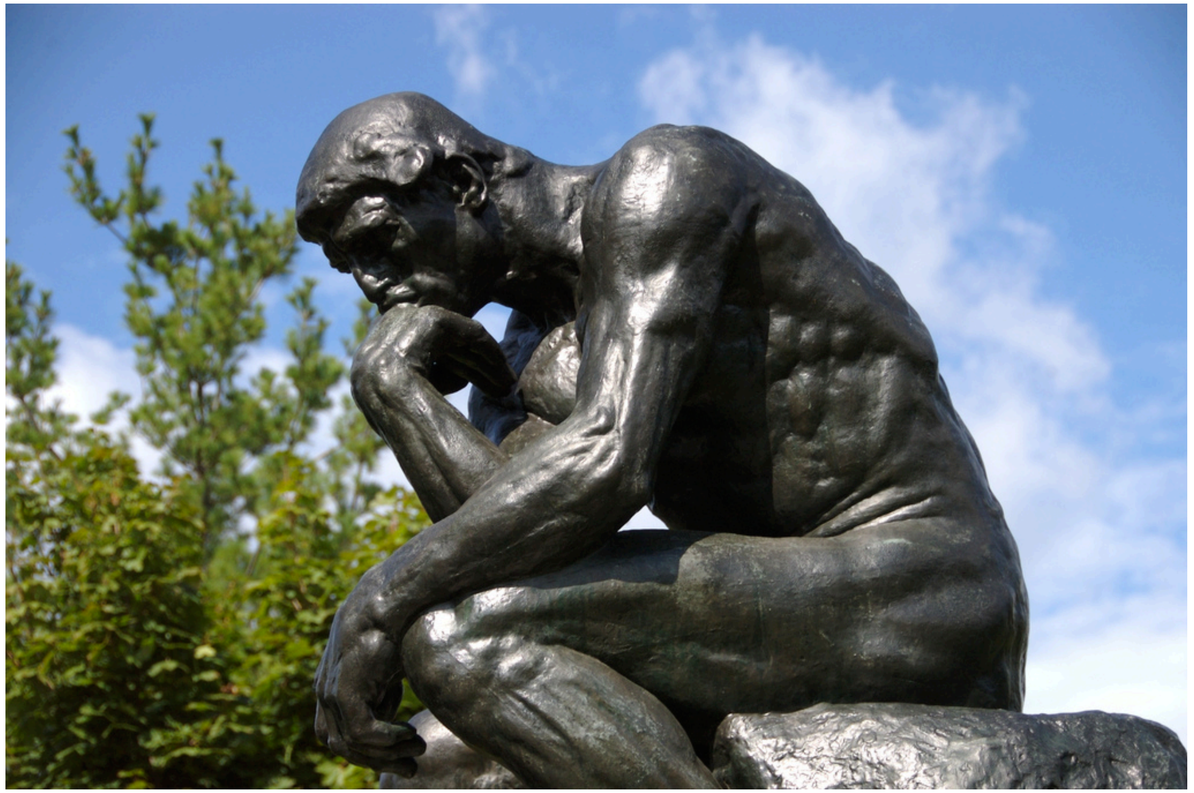
If security is considered between "slog" and "launch", will it be prioritized?
What wins: speedy, sufficient, or secure?

HOW TO MEASURE CULTURE *(FEEDBACK)*

Let’s Make a Cultural PACT

Which values are most key to your business strategy:
Process, Autonomy, Compliance, or Trust?

Ask Yourself

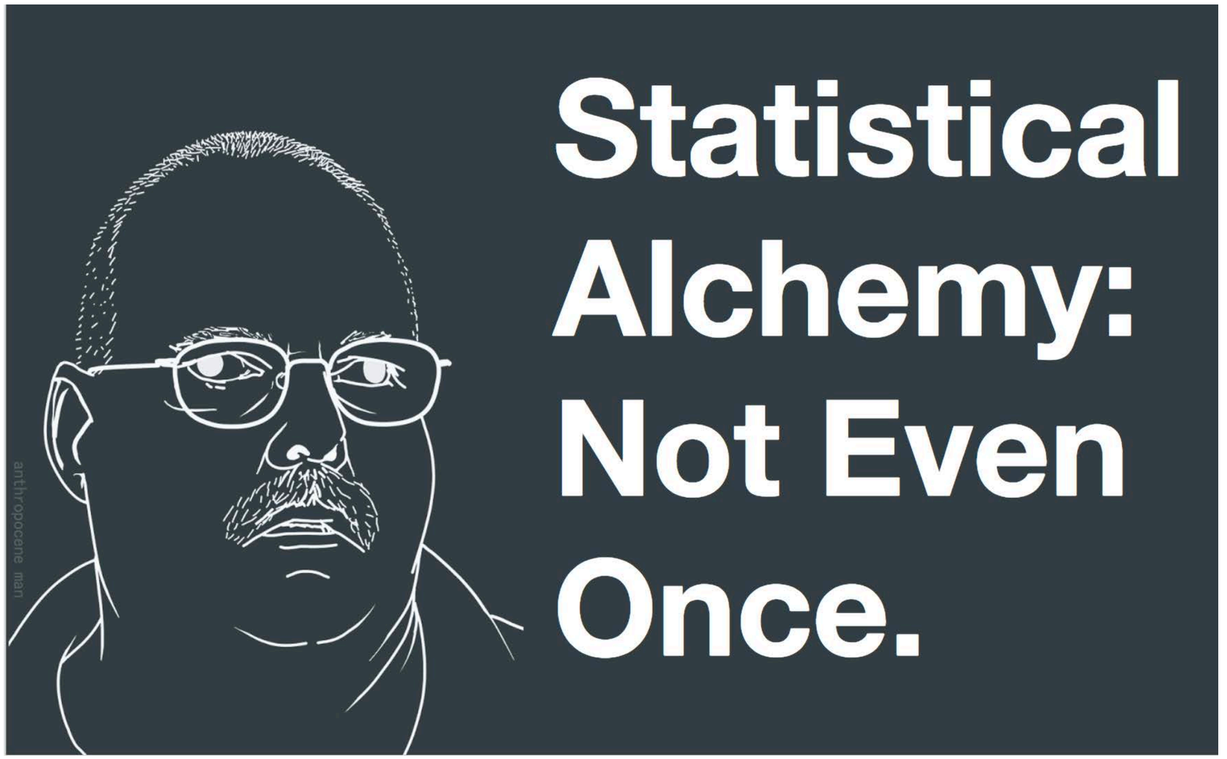


- What's most valued? What's rewarded?
- How do we measure risk? Accountability?
- How is security communicated and documented? What is stressed?

Ask Your Users

- W.W.U.X.D.?
- Where does it hurt?
- Which parts of our history are we (currently) doomed to repeat?

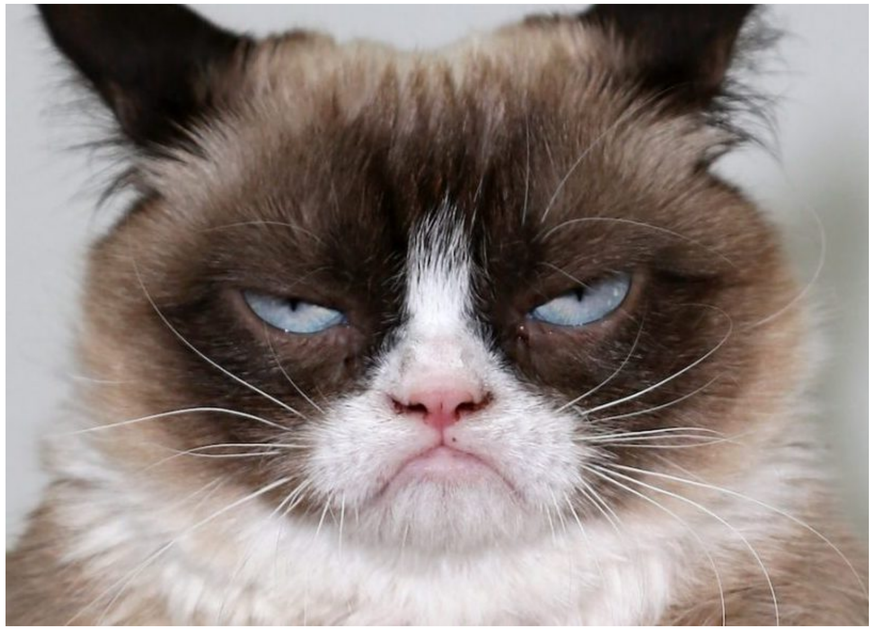
A Note On “Soft” Data

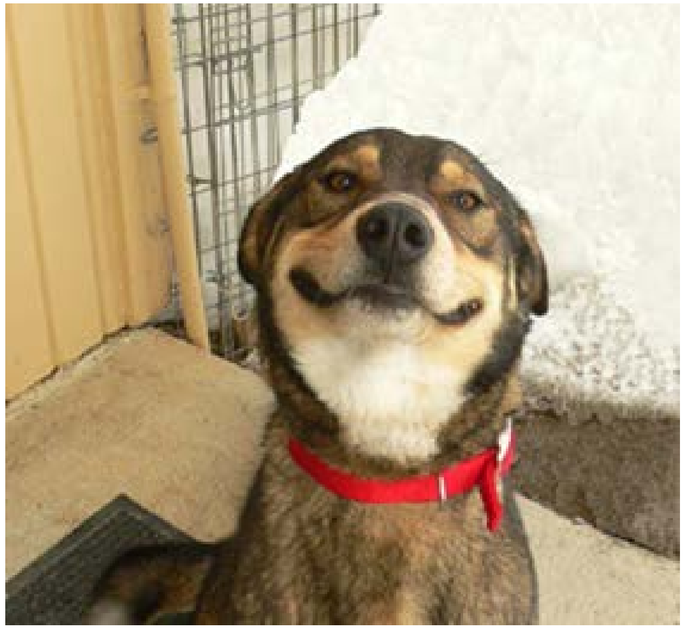


Data is like a kiwi: even if it’s fuzzy, it can still be useful.

WHAT INFLUENCES CULTURE?
(INPUTS)

How Good Is Your User Interface?



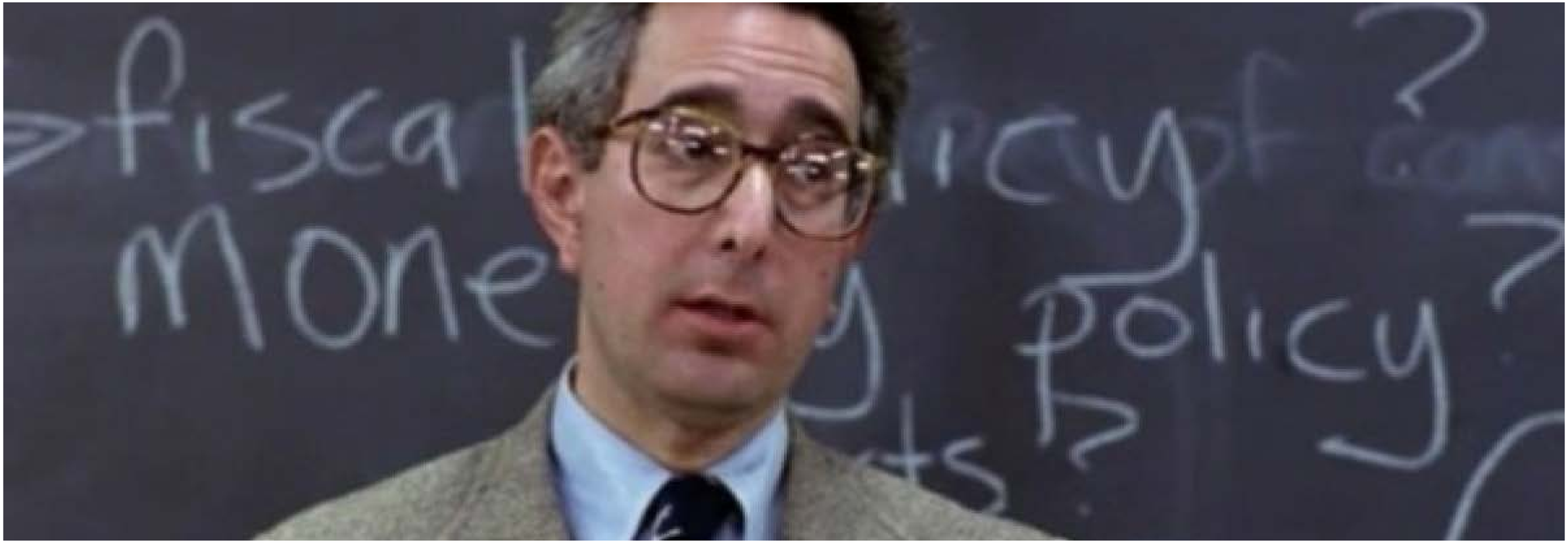


Which security critter would YOU bring a question to?
Which would you avoid?

Education: User Patching

- Start with respect, not roadblocks
- Continuous delivery over infrequent milestone updates
- Right-size the instruction for the user's understanding level

Education: User Patching



Caption

Teach. Differently.

- Vary teaching method for different learning styles
- Avoid lectures, increase engagement
- Give them ways to win

Application: All that's nice, now what?

- **Next week** you should:
  - Collect historical data on security comms (help desk tickets, security notices, incident reports, etc.)
  - Sketch user personas based on top role, seniority, and top priorities
  - Self-assess using Security Culture Diagnostic Survey *(available for download at lancehayden.net/culture)*
- **In the next three months** you should:
  - Identify top 2-3 processes needing improvement based on historical review
  - Choose users representative of each persona to survey. Along with SCDS (quantitative), conduct qualitative (Q&A) survey focused on top processes to pinpoint revision opportunities
  - Set revision target benchmark ("reduce help desk tickets related to [x] by 30%"), solicit feedback on proposed revision, beta test with user group to compare
  - Compare benchmark performance to goal, iterate or identify next process
- **In six months** you should:
  - Document iterated process, schedule repeat survey with larger sample group of users for each persona on schedule (annual/bi-annual/quarterly as appropriate).
  - Consider both risk reduction and cost/labor savings metrics for executive buy-in, and top win stories/kudos for users to communicate improvement value