RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: HUM-T07

The Art of the Nudge: Cheap Ways to Steer User Behavior

Dr. Branden R. Williams
Director, Cyber Security
MUFG Union Bank, N.A.
@BrandenWilliams

Behavior Guidance/Manipulation old as time

- How do I get a person to make my preferred choice when presented with options?
- Perhaps as old as the concept of the transaction itself!
- Sam Walton knew this (stick a pallet of Moon Pies out front, put them on special, YOU WILL SELL LOTS OF MOON PIES).

Some simple scenarios

- Buy my product, or walk away (nudged into doing the transaction).
- Buy the specific VERSION of my product that pays me best (nudge into a particular bundle/mix).
- Perhaps act in ways that maximize my payoffs, at odd with ethics (Wells).
- Play on bias/guilt to nudge you into a preferred choice:
  - Conservation (energy/water)?
  - Low calorie meals (dressing on the side)?
  - Healthful choices (fruit/candy)?

RSAConference2019

What the heck is a nudge anyway?

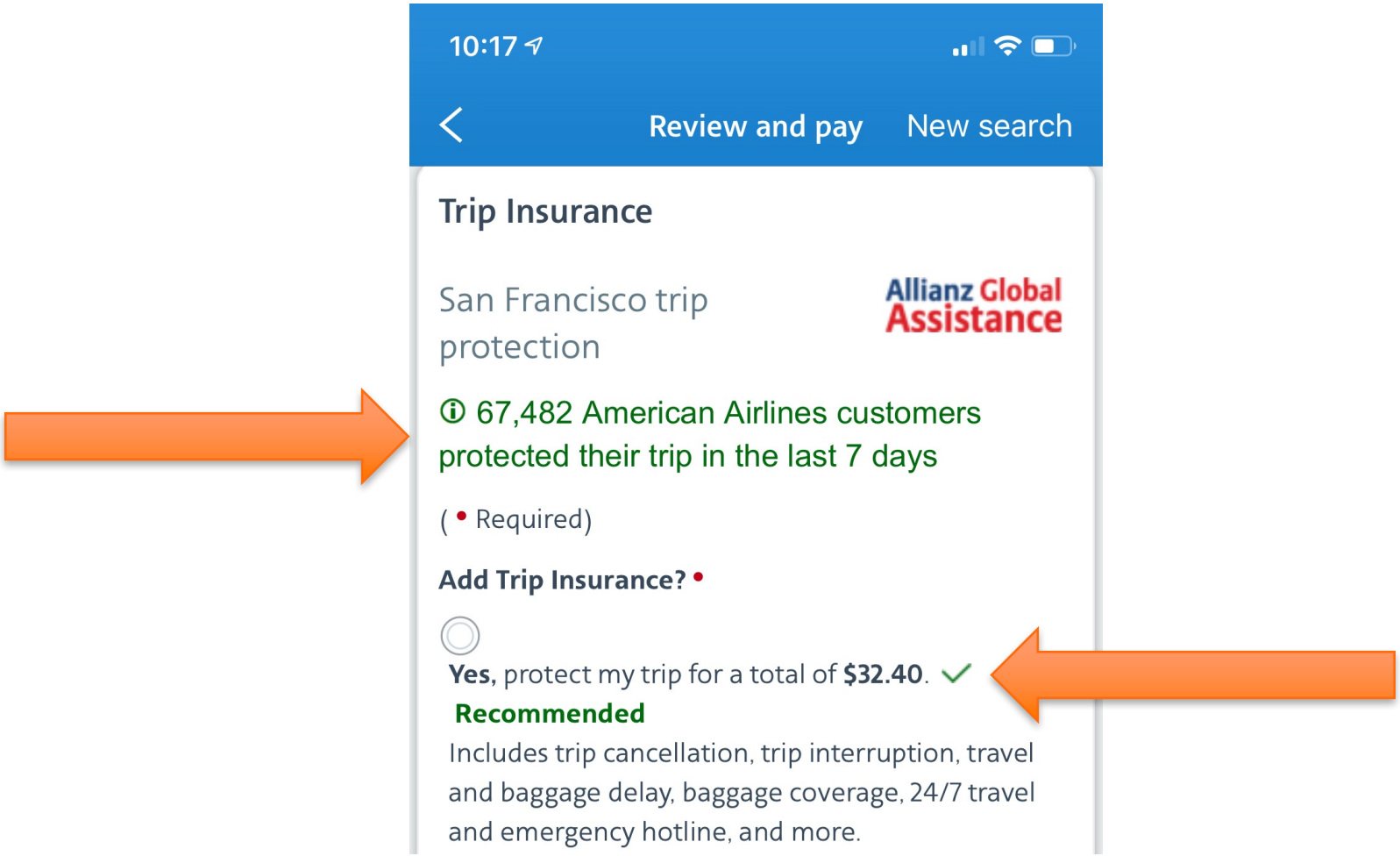
Defining the nudge

- A nudge is a technique codified from almost **100 years of behavior economics research and theory**.
- It's a way to take advantage of **subtle or even subconscious bias** to encourage someone to choose a path you, the choice architect, prefers (versus what the subject may prefer).
- Definition is changing as scholars research and contribute to the literature, **but most agree on the following tenets**:
  - Produces predictable outcomes.
  - Should favor the better or more rational decision.
  - Should exploit the individual's cognitive bias, routines, and habits.

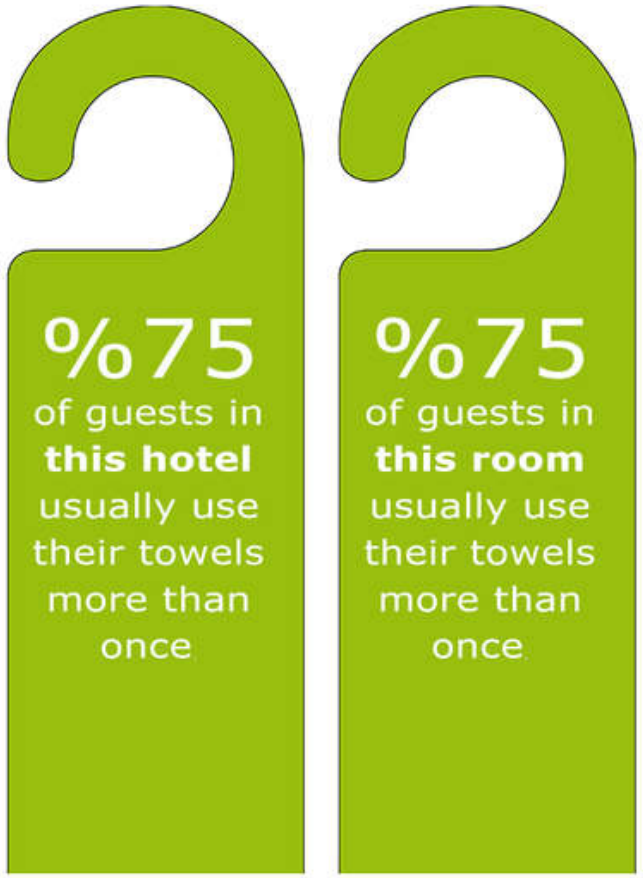
Nudge Theory

- Popularized by Richard Thaler and Cass Sunstein's book: Nudge: Improving Decisions about Health, Wealth, and Happiness
- Codified the framework that everyone can use.
- In use in both private enterprise and public policy.
- Payment network's EMV Liability Shift, GREAT example.

Examples of nudges



Examples of nudges



Examples of nudges

Example of a nudge for good

Example of an evil nudge

Decoys (Famously from The Economist)

Economist.com Subscription	Economist.com + Economist Print Subscription
$59	$125

Decoys (Famously from The Economist)

Economist.com Subscription	Economist Print Subscription	Economist.com + Economist Print Subscription
$59	$125	$125

Why should we care?

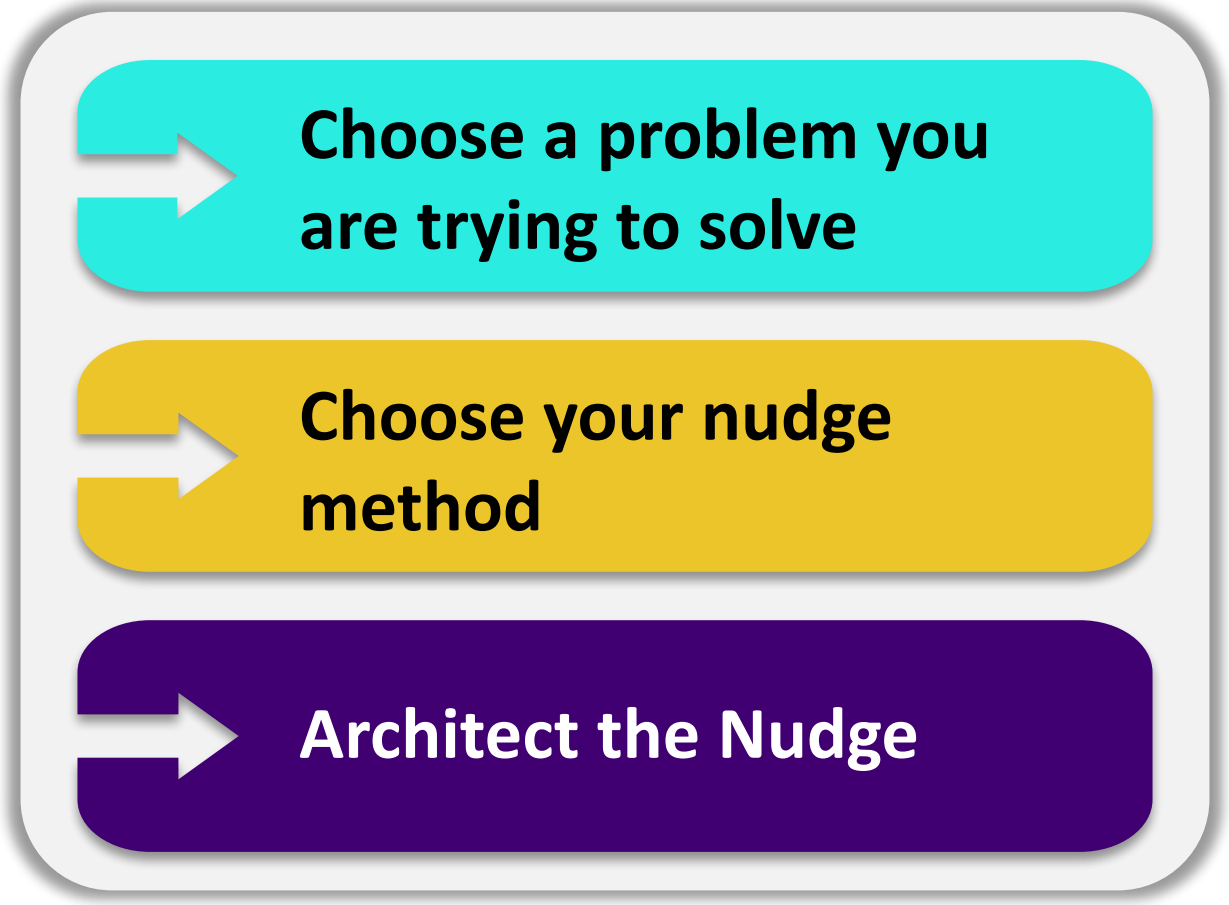
Why should we care?

- Nudges happen all around us. Awareness is half the battle!
- Learning which ones are effective directly translates to information security nudges.
- They are a FREEEEEEEEE (for the most part) security control.
- Becoming a better choice architect will improve your security function's performance directly without increasing cost.

Methods for Nudging

- **Simplification** (make information more straightforward and easy to process) and **framing** (phrasing of information to activate values/attitudes of target) of information.
- **Changes to the physical environment** to guide your target to one choice over another.
- **Changes to the default policy** such that the standard choice is the one you want them to make.
- **Use of social norms** to leverage peer pressure to cause your target to choose the preferred option.

Nudge Framework



Step 1: Choose a problem to solve

- People printing out confidential information and leaving it on their desks while they go to lunch.
- Leaving a workstation unlocked while you go to the breakroom.
- Emailing confidential information to someone not authorized to view it.
- Stopping people from clicking on a bad link that causes malware to be installed.

Step 2: Choose your method

- **Simplification** (make information more straightforward and easy to process) and **framing** (phrasing of information to activate values/attitudes of target) of information.
- **Changes to the physical environment** to guide your target to one choice over another.
- **Changes to the default policy** such that the standard choice is the one you want them to make.
- **Use of social norms** to leverage peer pressure to cause your target to choose the preferred option.

Step 3: Architect the nudge

- **Social Norms:** Prompt user to not print, remind them that paper breaches hurt too, make them click “I Acknowledge” to continue.
- **Changes to the Physical Environment:** Posters outside cubes reminding people to lock workstations.
- **Change the Default Policy:** Instead of automatically sending the email, use keyword searches to alert the sender that the email may contain confidential information, and to check the recipient.
- **Framing:** Alert the user that the email is EXTERNAL and they should not click the links.

Examples

- **Local Admin Requests:** Increase documentation requirements and approvals, extend SLA, require charge code. As an alternative, offer a one hour discovery session (free) where a colleague can help the user do their job without Local Admin. (DEFAULT POLICY, PHYSICAL ENV)
- **Badge-Out Policy:** Enforcing a Badge Out policy to nudge against tailgating. A side benefit is added data that we can use on understanding “Day In The Life” of employees. (DEFAULT POLICY)
- **Reducing Waste/Risk via Printing:** Charge back users for pages printed or require 100 word justification for what is being printed at printing time. Requiring a justification would replace a charge and would make users think before printing. The result should be decreased printing of [sensitive] information, which could lead to decreased information leakage from hard copies being left unattended or lost. (DEFAULT POLICY)

Examples

- **More Printed Materials:** Sign on conference or meeting rooms if not already in place “Remember not to leave any presentation material behind, if no longer required ensure it’s disposed of properly in special shredding bins.” (FRAMING)
- **Workstation Locking:** Signs in the hallways on the way to the bathroom, kitchen, coffee area, elevators. “Hey have you locked your workstation?” (SOCIAL NORMS)

Review/Summary, We Made It!

- Nudges can be used as a cheap or free security control that encourages your fellow employees (or customers!) to choose the secure pathway.
- Nudges should:
  - Produce predictable outcomes.
  - Should favor the better or more rational decision.
  - Should exploit the individual's cognitive bias, routines, and habits.
- And Leverage:
  - Simplification and framing of information.
  - Changes to the physical environment.
  - Changes to the default policy.
  - Use of social norms.

Apply what you learned today

- Next week you should:
  - Identify 3-5 human security problems that are worth solving
- In the first three months following this presentation you should:
  - Pick one or two of those problems and fully define/understand it
  - Architect a nudge to subtly have humans correct their own behavior
- Within six months you should:
  - Evaluate the results of your nudge and iterate if required
  - Choose another problem to solve, Deputy Choice Architect!

Questions/Answers/More Info

- BRING THOSE QUESTIONS!
- If you want to learn more:
  - Send a blank email to b@SendYourSlides.com
  - With the subject: rsac2019
- Tweet me: @BrandenWilliams
- http://blog.brandenwilliams.com/