BUT, I'M NOT A TARGET!
HOW TO COMBAT THE HIDDEN BIAS THAT KILLS YOUR AWARENESS PROGRAMME

JORDAN SCHROEDER, CISSP, CISM
WHO AM I?

- Senior Security Consultant for ECS
- Author of “Advanced Persistent Training: Take Your Security Awareness Programme to the Next Level”
  - [AdvancedPersistentTraining.com](http://AdvancedPersistentTraining.com)
  - [GoPhishYourself.co.uk](http://GoPhishYourself.co.uk)
- Designed the SelfPhish awareness research platform
- Former teacher, actor, singer, director, playwright, Coast Guard Officer, undertaker, database designer, tax preparer, business owner, day trader
INTRO

SET THE SCENE

- Risky behaviour, meet Risky consequence
KNOWLEDGE IS NOT ENOUGH
KNOWLEDGE IS NOT ENOUGH

“it won’t happen to me”
NEAR-MISS BIAS
NASA COMMISSIONED STUDIES

2008

Robin L. Dillon, Catherine H. Tinsley
McDonough School of Business, Georgetown University, Washington, D.C. 20057

2012

How Near-Miss Events Amplify or Attenuate Risky Decision Making
Robin Dillon-Merrill, Catherine H. Tinsley, Mathew A. Cronin
McDonough School of Business, Georgetown University, Washington, D.C. 20057
WHAT IS IT?

COLUMBIA SHUTTLE DISASTER 2003

Foam Debris
WHAT IS IT?

COLUMBIA SHUTTLE DISASTER 2003
WHAT IS IT?

THE EXPERIMENT

- Information Management Business students (with training in stats and probabilities) put through a simulation where they have to navigate the Mars Rover from one crater to another.

- Each simulated day, given a weather report, the participant needed to decide to stay or move on given the weather’s chance of causing a wheel failure.

**NASA EXPERIMENT**

- Those who ‘survived’ the risky choices were more prone to making riskier decisions for the next day.

- Even when presented with the probabilities afresh each day, participants still incorporated the previous successes into their decisions, **even if** they did not make as many risky decisions.
  
  "I know I survived last time, but … “

- *When given the choice of knowing Near-Miss data or other data, participants were less likely to seek other data*
WHAT IS IT?

NEAR-MISS

- People tend see events as linked and not independent
  - "hot streaks"
- People with Near-Miss information tend to skew towards riskier decisions

NEAR-MISS DATA = SECRET SAUCE

- Near-Miss data incorporated with statistical data
  - Like a secret ingredient
  - “My successes were because the probabilities were general and not applicable to my specific situation. My probabilities are different.”
  - (Stats) + (Near-Miss adjustment) = expected probability
  - Version of the Gambler’s Fallacy
MISS - COMMUNICATING
NEAR-MISS COULD BE INTERPRETED TWO WAYS

- Disasters that did not occur
  - **Resilient Risks**
    - “Yay! I didn’t die!”
- Disasters that almost happened
  - **Vulnerable Risks**
    - “OMG! I almost died!”

RESILIENT RISKS

- Results in riskier behaviours
- Reduction in mitigating behaviours
- Explicit Likelihood calculations do not change
  - quietly ‘enhanced’ with a hidden calculation when there is a call to action

THE HIDDEN CALCULATION

- You present your risks
- You present your calculations
- Your audience agrees with it all
- Your audience quietly applies their own Near-Miss factor
- *Then* your audience decides
  - budget, personnel, InfoSec projects, etc.
PRESENT VULNERABLE RISKS INSTEAD

If Near-Miss information is communicated as **Vulnerable Risks**, (“we almost died!”):  

- and if the audience accepts that framing  
- the effects of Resilient Risks are countered  
- more mitigating behaviours are used

MISS - COMMUNICATING

VULNERABLE CHALLENGES

- The audience might not accept your framing
  - becomes a messaging/relationship/trust issue
- Creates a tone of negativity (less fun, less value)
  - The mitigations become devalued!
- The messenger becomes devalued!

COMMUNICATING RISK

- Focus on the Probabilities
  - Frame past events as independent and not a chain
- Focus on the potential impact
  - Frame Near-Misses as Vulnerable Risks
COMMUNICATING RISK - JORDAN

- Focus on Procedural Resiliency
  - Combat Vulnerable Risk negativity by celebrating the resiliency of protections
  - “Yay! We are surviving because we are using the right people, processes, and tools!”
- Make insurance sexy
COMMUNICATING RISK - JORDAN

- Communicate vulnerability:
  - How many infections this year
  - Number of uncaught malicious emails that slipped thru

- Communicate effect of process
  - The people who communicated infections as soon as possible saved us X investigation hours
  - Y% of malicious emails had obviously fake links
EXAMPLE IN SECURITY AWARENESS

- A/V caught a virus in an email attachment
  - not executed, no actualized risk
- Every once in a while, treat it as though it was an actual infection
- Run the Incident Response process
  - great training for new members
- Identify all vulnerable areas that were involved
SUMMARY
**NEAR-MISS BIAS**

- Past events seen as linked
- Near-Miss data is used to silently adjust probabilities
- Near-Miss data is preferred over other data
- Used to justify riskier behaviours
SUMMARY

COMMUNICATING NEAR-MISS

- Focus on Probabilities
  - De-link events
- Focus on potential harm
  - Shift to Vulnerable Risks
- Focus on Procedural Resiliencies
  - Combat negativity
THANK YOU