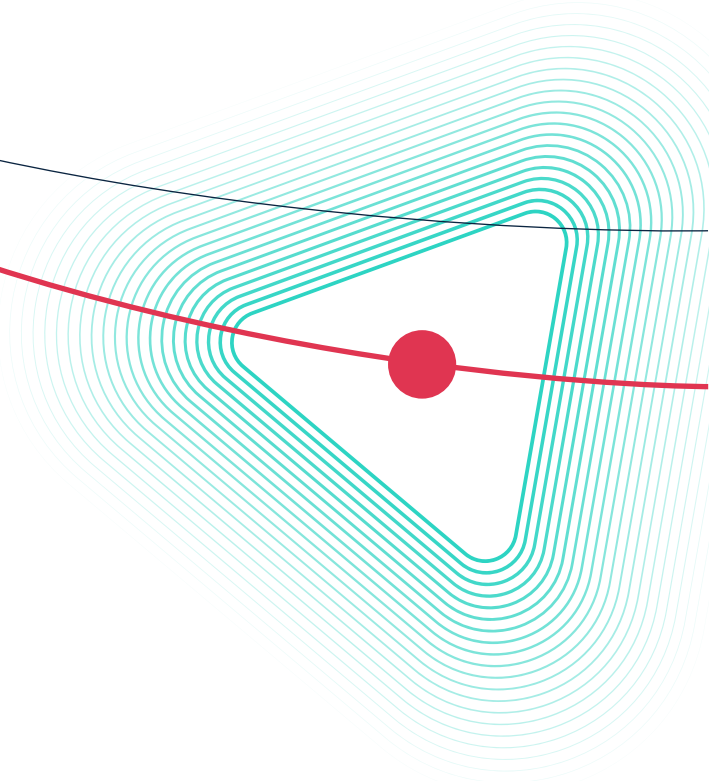
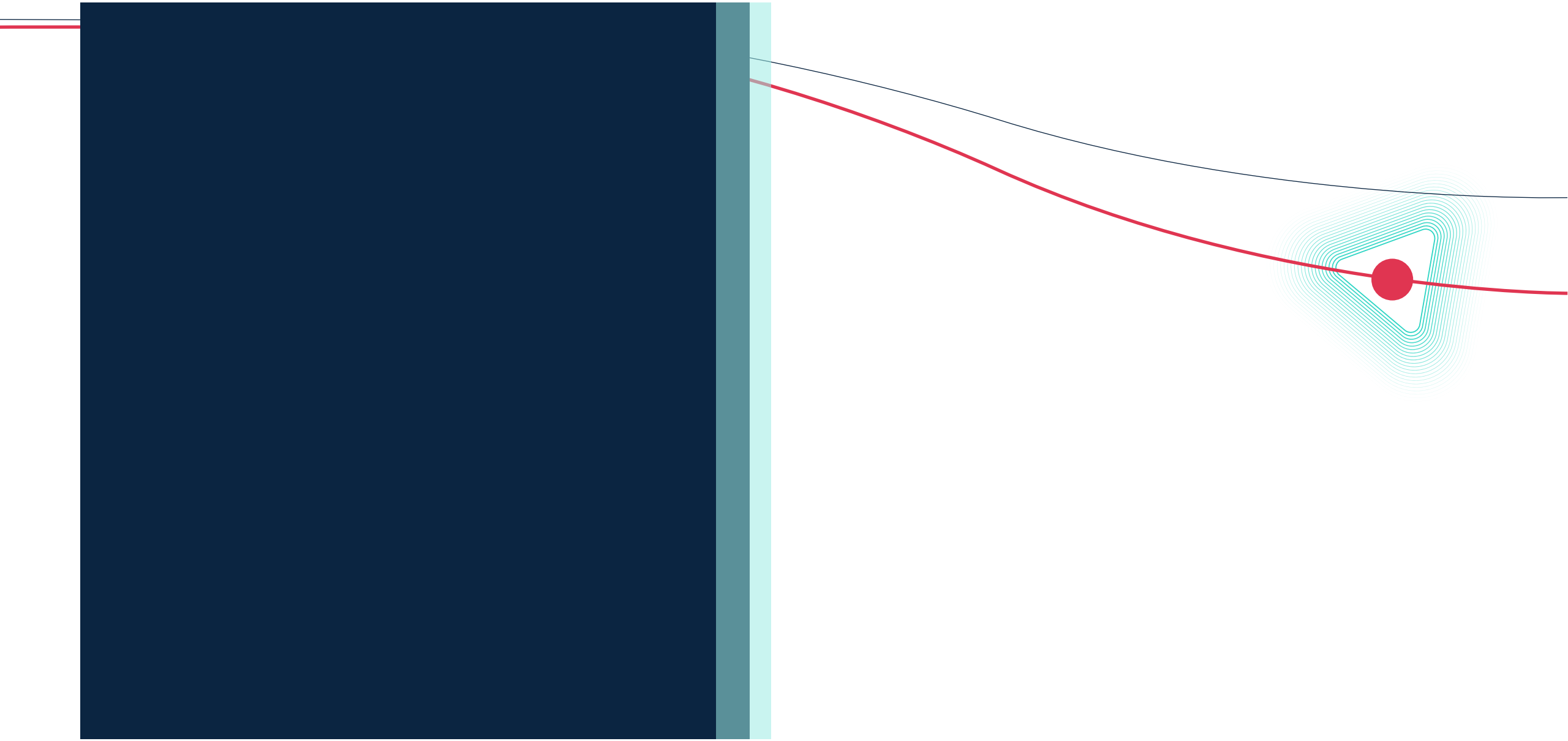
CYE

Human Security Engineering:
Stop relying on the failed human firewall



Ira Winkler, CISSP



A Highly Sophisticated Attack

17 Year Old Mastermind

- Lots of social engineering
- Determined location of admin tools
- Conducted Vishing attacks
- Accessed tools that 1,000 people had access to

”A Problem of Leadership”

CLOUDFLARE®

Old School Safety Science

- Why did the user do what they did?
- Focus on the proximity of the error
- Analysis of why user was wrong

Operational Problems

- Proximity doesn’t explain a lot

  Mechanical breakdowns?

- Medical post-mortems

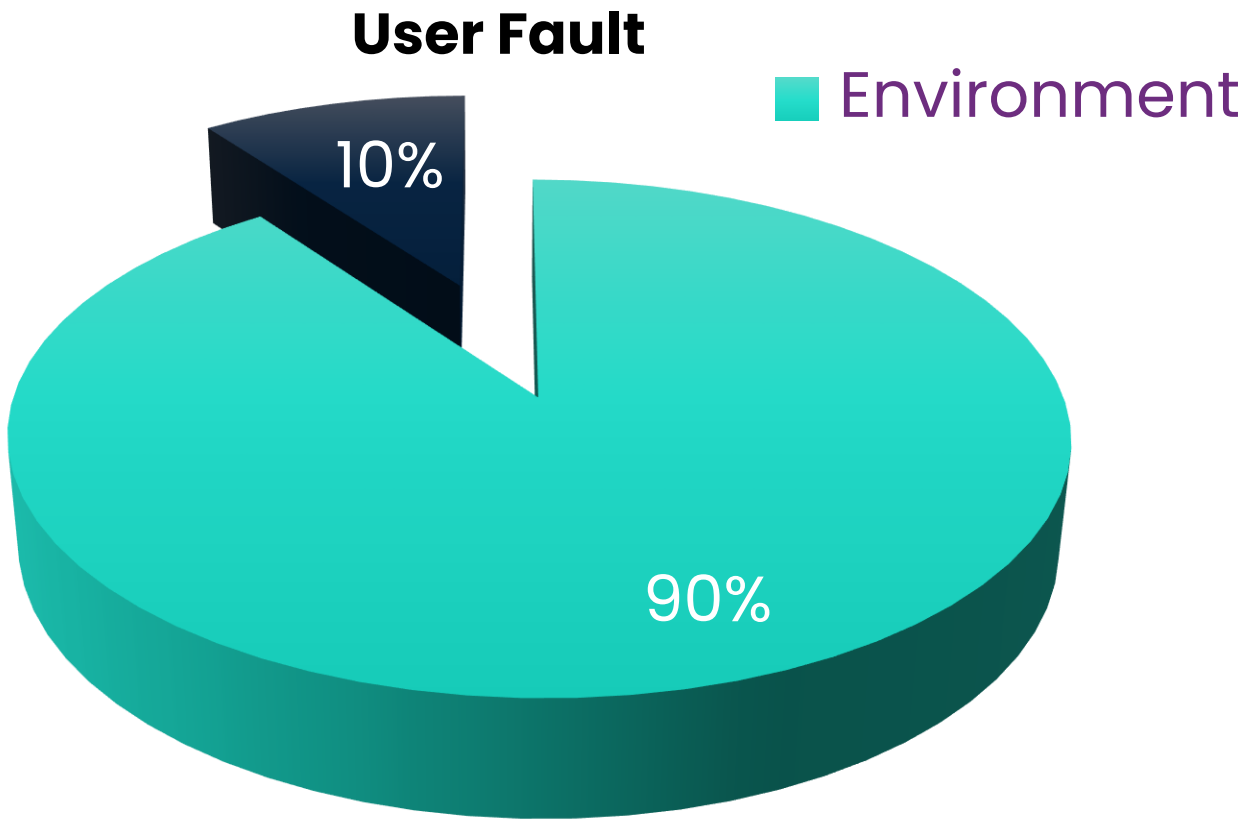
  One bad actions results from hundreds of complex decisions

New School Safety Science

- A user is as much a part of the system as a computer
- Any safety incident results from a failure of the entire system
- Review all enabling factors
- The user is just the proximity of the error
- Proximity is just a symptom
- User error is a symptom of what is wrong with the system


(c) Rich Galiano

Where Blame Falls



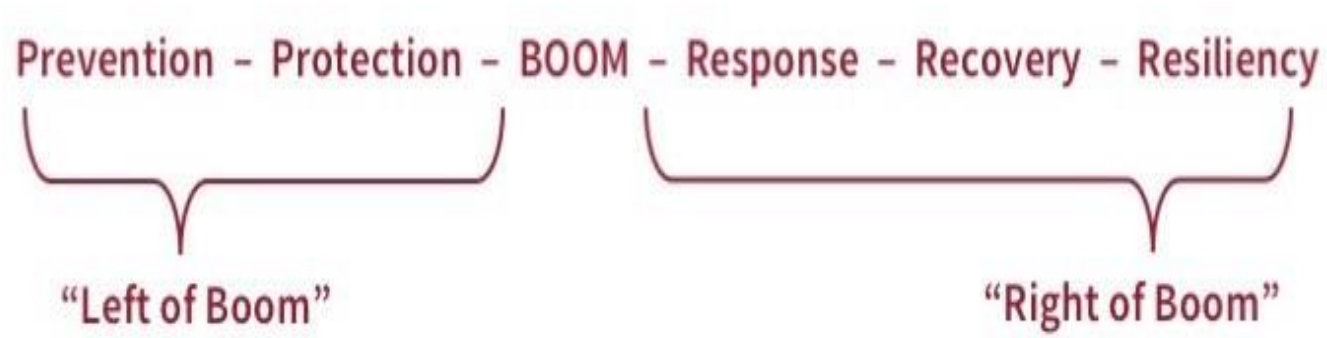
What is That 10%

- Carelessness
- Blatant ignorance
- Lack of training
- Malice
- This is where awareness and training might fit in, kind of
- Still only 10% of the problem

Let’s Talk Boom

What is Boom?

- A counterterrorism strategy
- Boom is the explosion
- “Move Left” origin



User Initiated Loss

- A user doesn’t cause damage or a loss

THE SYSTEM DOES

- A user action just initiates the loss possibility
- UIL can be ignorance, carelessness, system related, or malice
- Want to stop UIL potential
- Want to stop the actual UIL
- Want to mitigate loss after initiation

Left of Boom

- Prevent user from being in a position to initiate loss
- Take away decision or capability
- Prevent, Detect, React to attack targeting a user
- Create a Culture, aka Consequences, to assist
- Users may aid in detection

  Tailgaters for example

Governance

- Are all organizational processes clearly defined?
- Are user actions there by default, or are they an intended result of clearly defined processes?
- Think about this carefully

Boom

- The user is presented with the opportunity to initiate a loss
- Do they

  Do it?
  Detect it?
  Prevent it?
  Sound the alarm?

- Remember, it can be accidental, careless, willful, malicious, or forced

Policies and Governance

- Are user actions very specifically defined?
- Are all actions necessary?
- Are you relying on an organization filled with Elmer Fudds?

Right of Boom

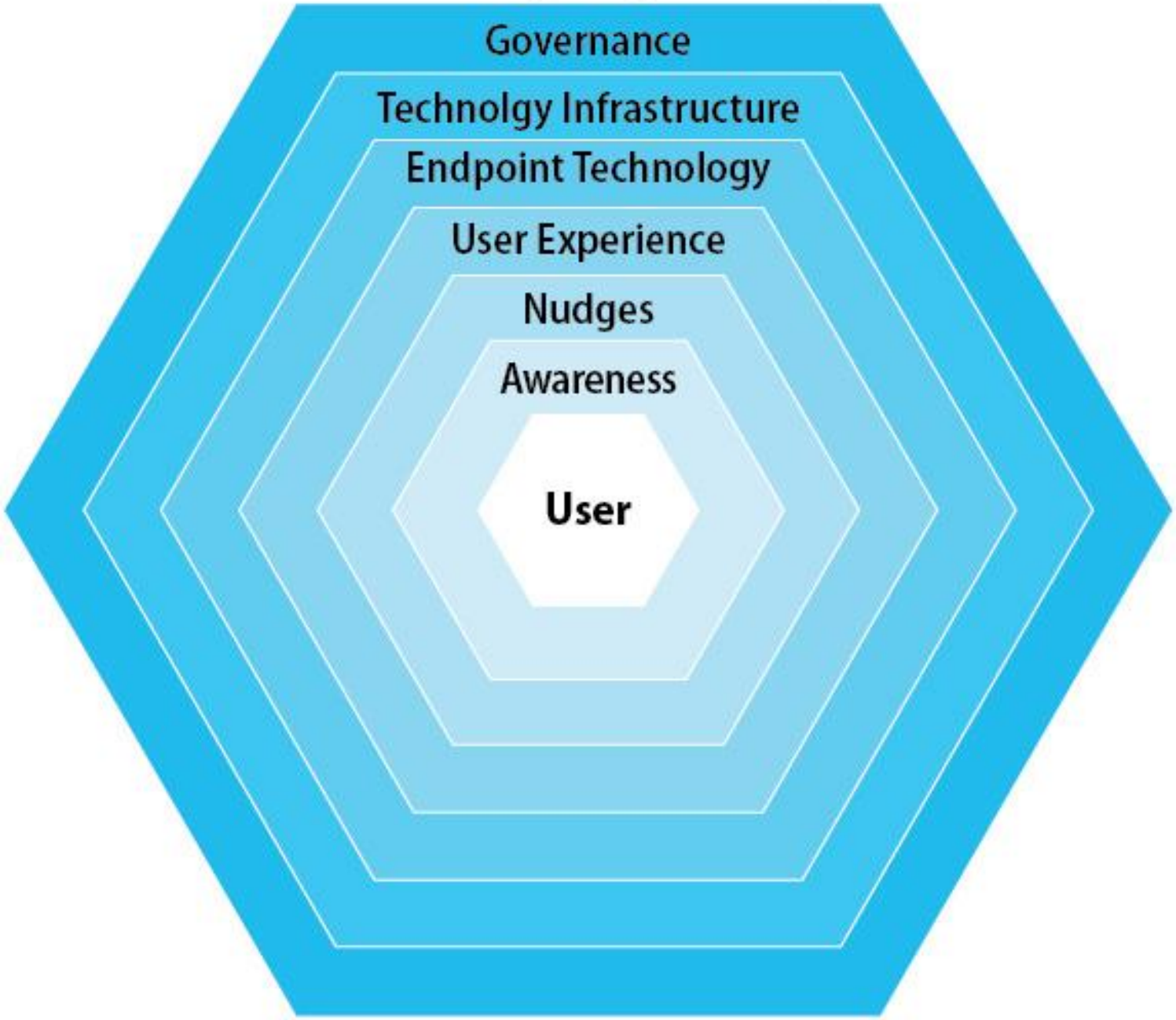
- Loss has been initiated
- Does the environment expect it?

  For example, users don’t have admin privileges

- Are there additional protections?
- Is there an analysis of UIL?

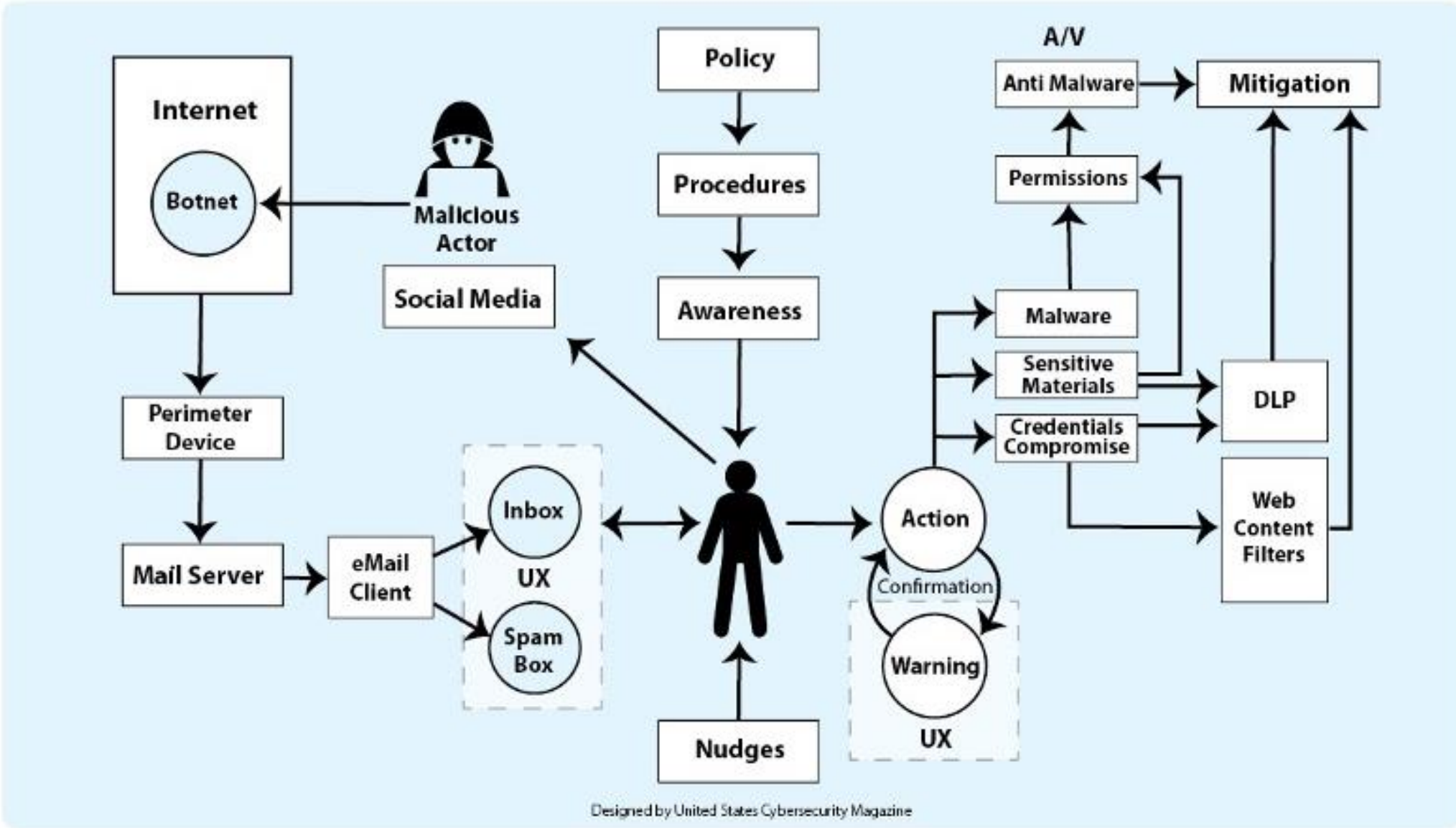
  What can users do?

Human Security Engineering Model

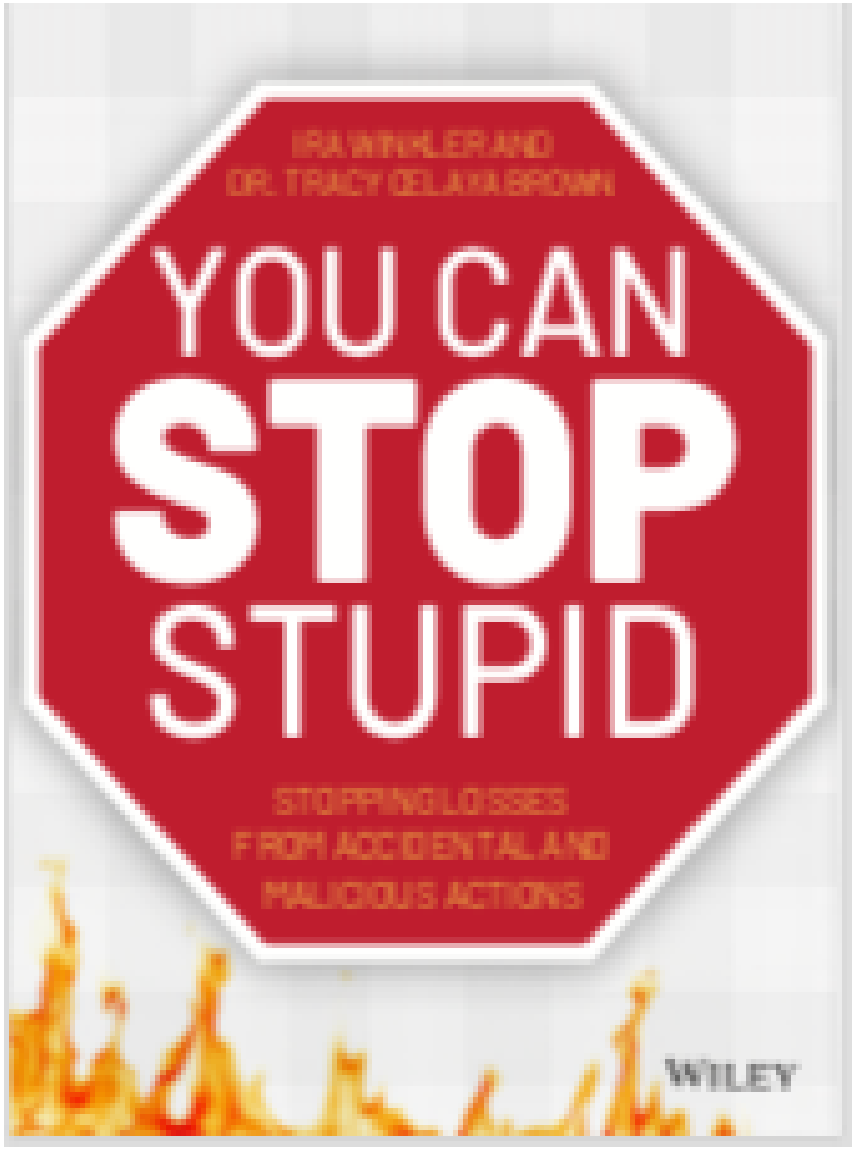


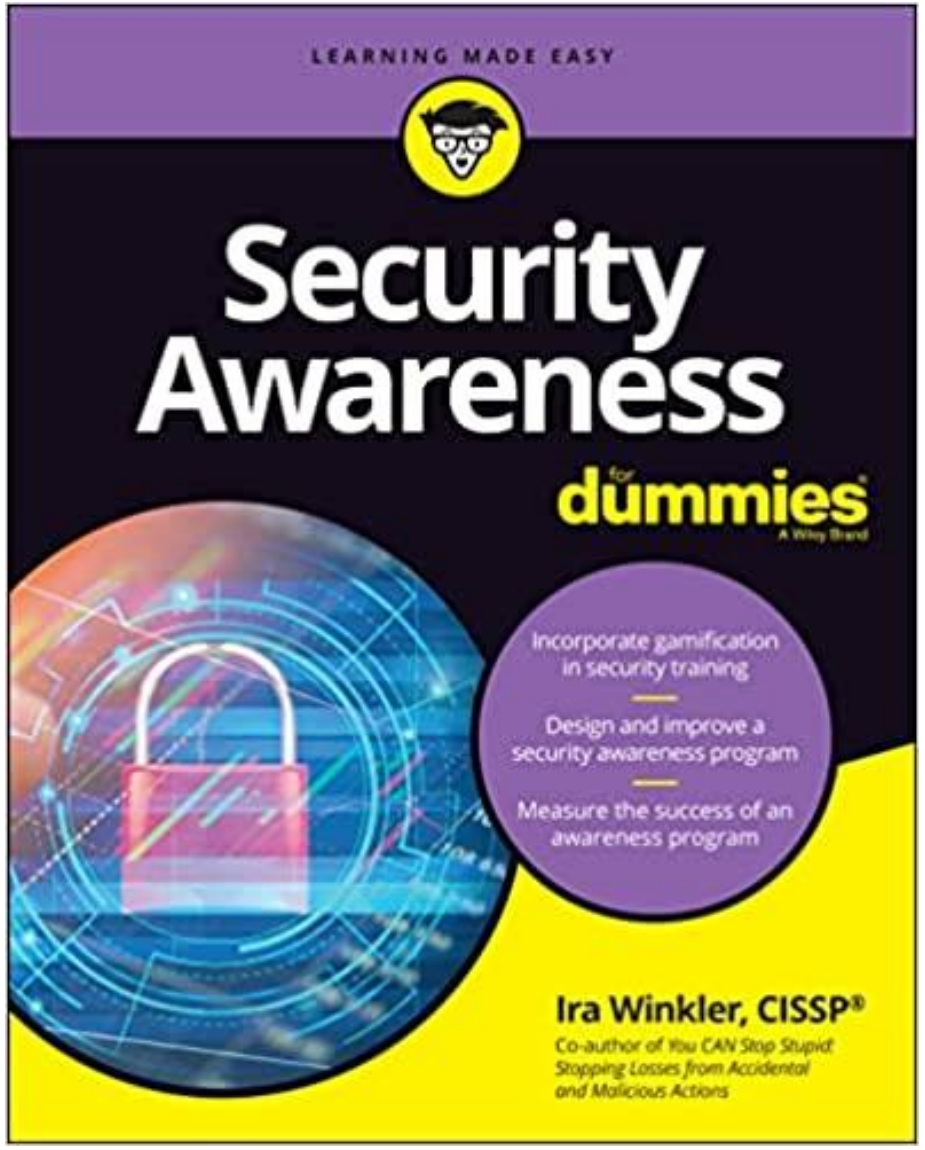
Designed by United States Cybersecurity Magazine

HUMAN SECURITY ENGINEERING MODEL PHISHING PREVENTION



The Most Important Takeaway


IRA WINKLER AND
DR. TRACY CELAYA BROWN
YOU CAN
STOP
STUPID
STOPPING LOSSES
FROM ACCIDENTAL AND
MALICIOUS ACTIONS
WILEY


LEARNING MADE EASY
Security
Awareness
for
dummies
A Wiley Brand
Incorporate gamification in security training
Design and improve a security awareness program
Measure the success of an awareness program
Ira Winkler, CISSP®
Co-author of You CAN Stop Stupid
Stopping Losses from Accidental
and Malicious Actions

Reach Out

Ira Winkler, CISSP

ira@securementem.com

https://www.linkedin.com/in/irawinkler

@irawinkler

https://www.cyesec.com