RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **KEY-F03S**

You Can Stop Stupid

Ira Winkler, CISSP

Lead Security Principal
Trustwave
@irawinkler

Dr. Tracy Celaya-Brown

President
Go Consulting International
@DrTre_C

#RSAC

What is Stupid?

Having or showing a great lack of intelligence or common sense

Do You Hire People with a Great Lack of Intelligence?

- Who’s fault is that then?
- Why did you put these people in a position of responsibility?

Do You Hire People Without Common Sense?

- You can’t have common sense without common knowledge
- Are you giving people common knowledge?
- Did you give people training?
- Did you expect the failing
- It’s common knowledge that people will eventually fail

So, Who’s the Stupid One?

It’s Not Really You

- You’ve been fed a bunch of ignorant crap
- The Human Firewall
- The users are your last line of defense
- The users are your first line of defense
- Lots of Broscience from people who read the wrong books

Focus on proximity of error

STRAIGHT
OUTTA
MOSCONE

Safety Science

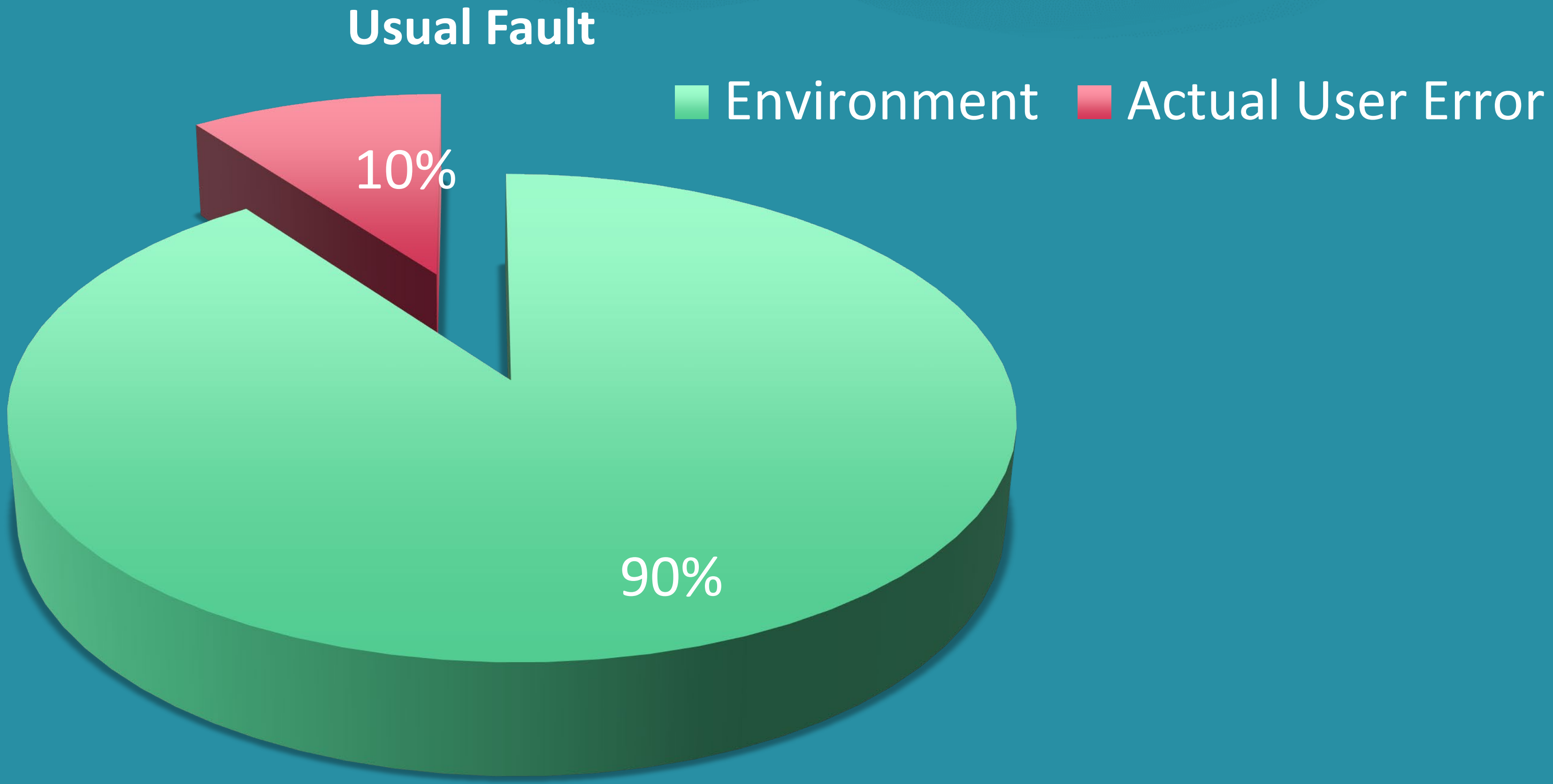
- A user is as much a part of the system as a computer
- Any safety incident results from a failure of the entire system
- Review all enabling factors
- The user is just the proximity of the error
- Proximity is just a symptom
- User error is a symptom of what is wrong with the system

Pilot Error?

Could Pilots Have Saved the Planes?

- Yes!
- But…
  - The cause was software and faulty sensors
  - They was improper training
  - They changed indicators
  - The problems were systematic and the pilots failed as part of they system

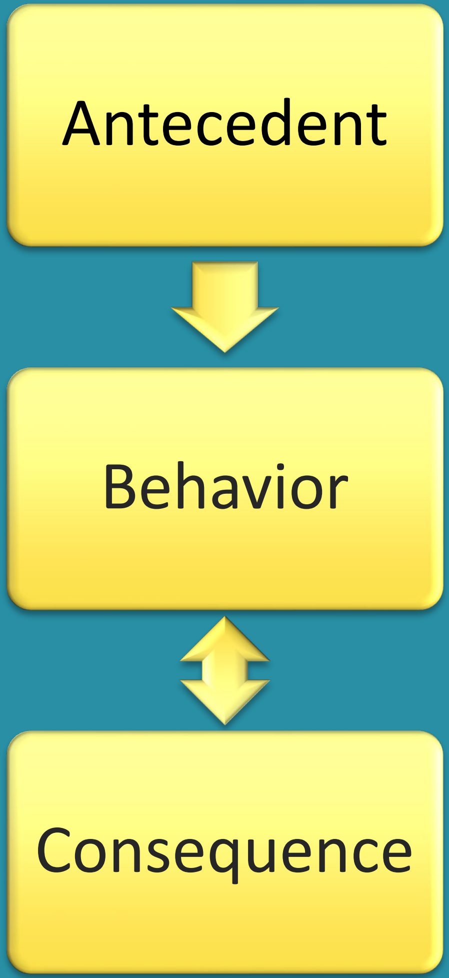
Where Blame Falls



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

Awareness is Only 20% of 10%

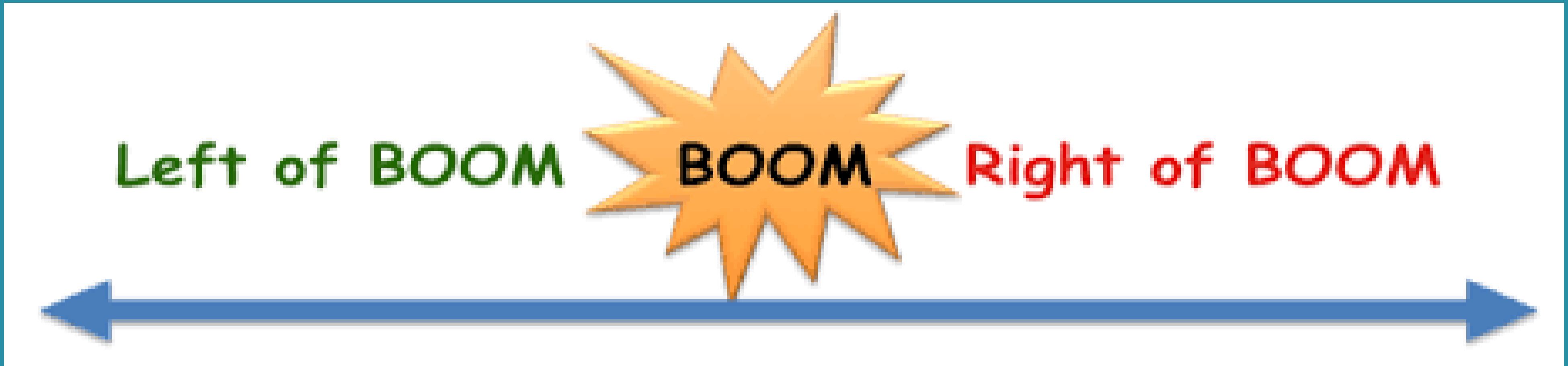


Antecedent

Behavior

Consequence

Let’s Talk Boom



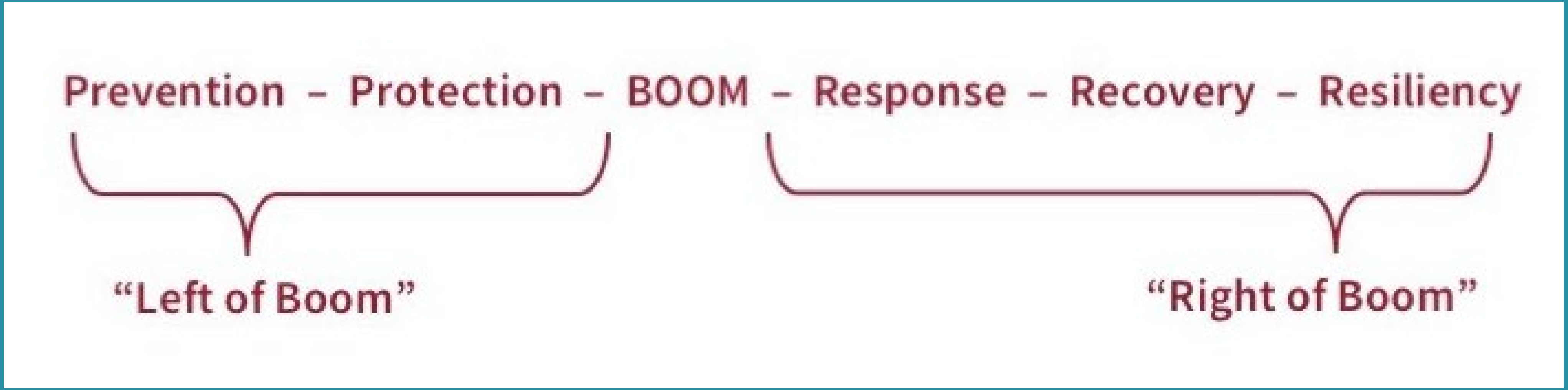
Left of BOOM

BOOM

Right of BOOM

What Is Boom?

- A Counterterrorism Strategy
- Boom is the explosion



Prevention – Protection – BOOM – Response – Recovery – Resiliency

"Left of Boom"

"Right of Boom"

Each Phase Involves Protection, Detection, and Reaction

- The canary is only involved at Boom
  - For the most part
- With 90% of attacks involving a user compromise, focus on Boom as a user action
- At each phase, you protect, detect, and react

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?

Most Important

- Go back and analyze the incident
- What caused the incident?
- What enabled the incident?
- Proximity is not the cause of the incident

Sounds Difficult, but…

- Safety science does this
- Accounting does this
- Operations does this
- Etc.

Consider This…

- If 90% of incidents result from some form of UIL, shouldn’t this, or a similar strategy, be used for your organizations?
- Do you currently analyze process, or just slap countermeasures around?

CEO W-2 Fraud Example

- Left of Boom
  - Mail filtering
  - Tagging of messages as external
- Boom
  - Process for release of PII
  - Training in the process
  - Reinforcement of the process
- Right of Boom
  - Warnings of attaching file
  - DLP software

Consider The Overlap

- Handling of PII vs warning of CEO fraud
- DLP for any types of attack
- Filtering of incoming email on servers
- Tagging of mail as external
- Warning of attachments

If you mitigate the 90% by robust countermeasures, won’t that take care of almost all of the remaining 10%?

Awareness is Still Mandatory

- What do you make them aware of?
- What to be afraid of or how to do things correctly
- In other words, awareness of proper procedures
- Some awareness and behavioral modification is also required
- Just don't focus on the general for your whole program

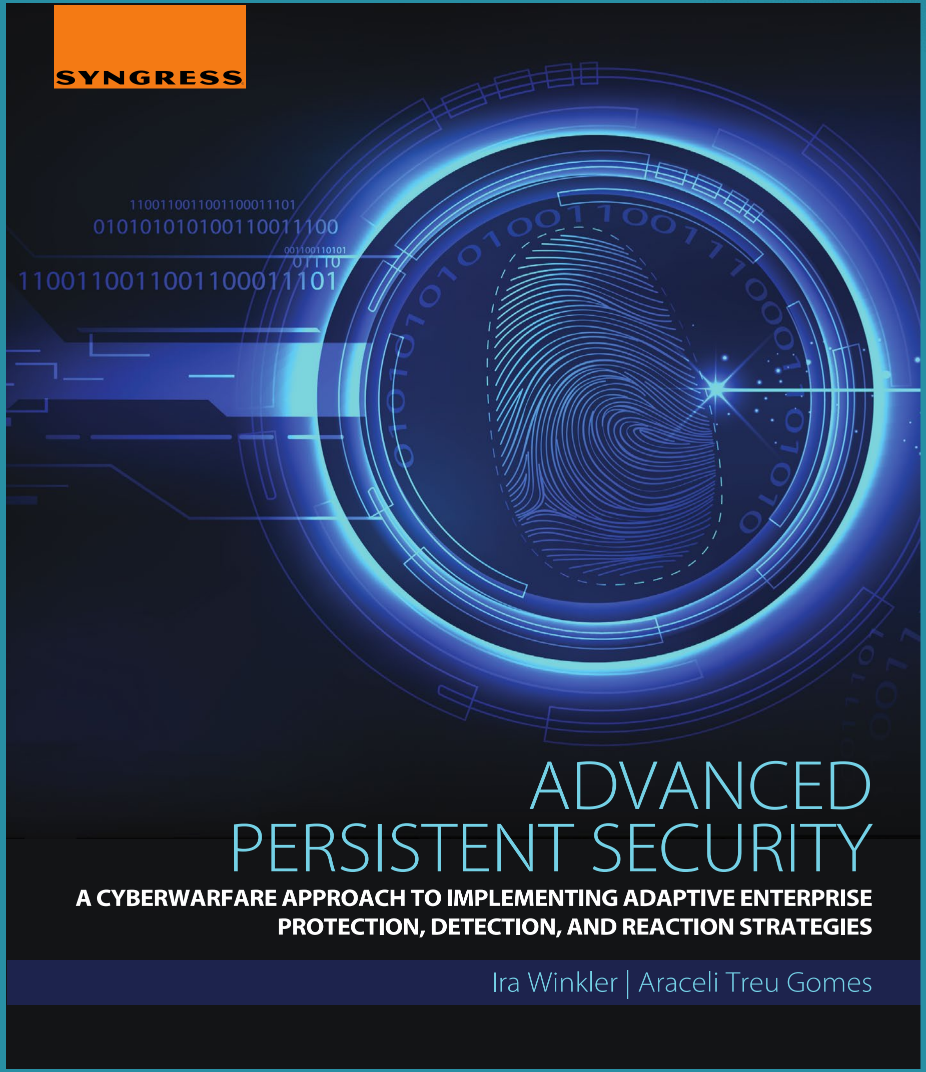
Are you throwing around random tactics to stop your greatest source of losses, or are you pursuing a strategy?

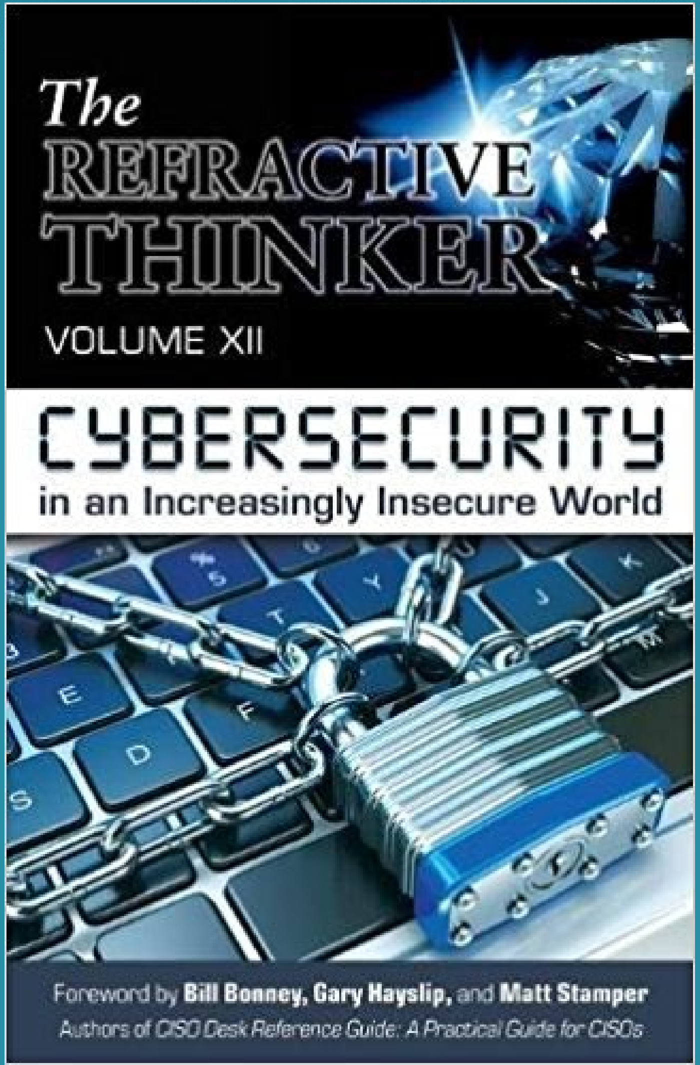
The Most Important Takeaway

“Apply” Slide

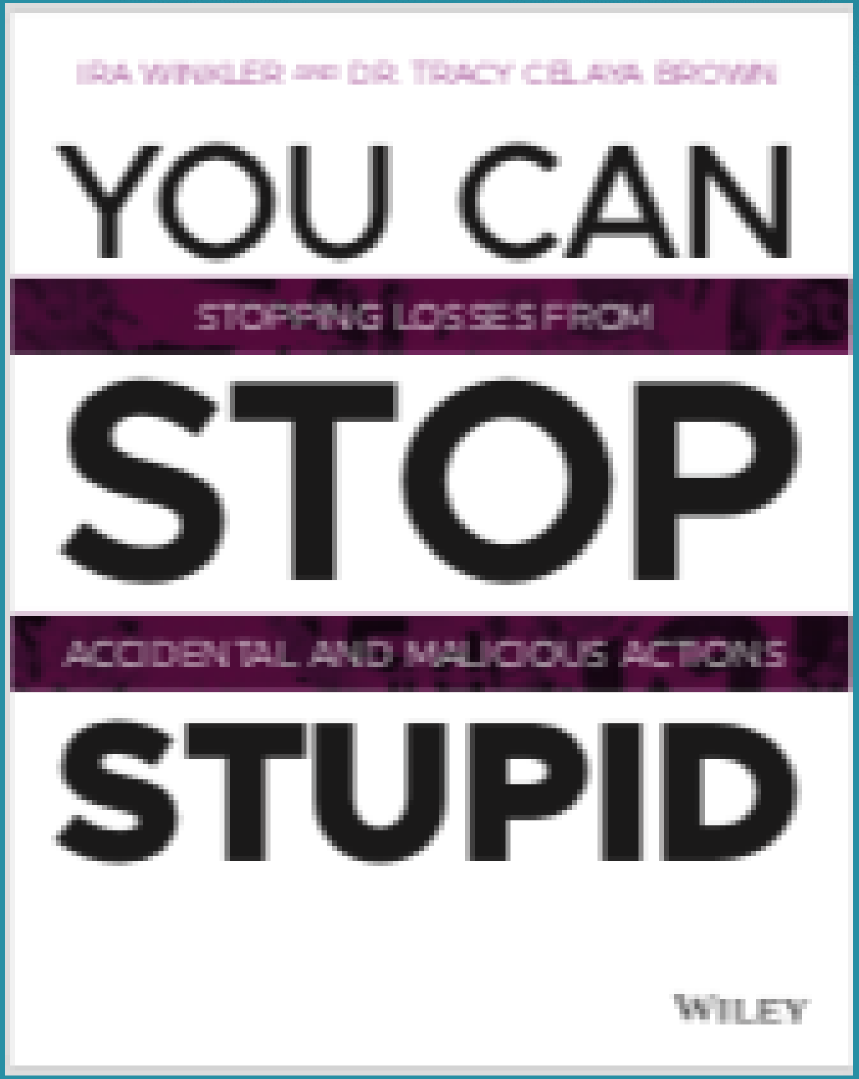
- Immediately
  - – Analyze Governance
  - – Do your efforts focus on error proximity?
  - – Is there an end-to-end approach for User Initiated Loss?
  - – Consider are you giving users “crap” to click on?
- Within 3 months
  - – Choose 2 common UILs to analyze
  - – Reevaluate the systematic issues
  - – Begin mitigation

The Books, The Myths, The Legends


SYNGRESS
ADVANCED PERSISTENT SECURITY
A CYBERWARFARE APPROACH TO IMPLEMENTING ADAPTIVE ENTERPRISE PROTECTION, DETECTION, AND REACTION STRATEGIES
Ira Winkler | Araceli Treu Gomes


The REFRACTIVE THINKER
VOLUME XII
CYBERSECURITY
in an Increasingly Insecure World
Foreword by Bill Bonney, Gary Hayslip, and Matt Stamper
Authors of CISO Desk Reference Guide: A Practical Guide for CISOs

Your Input?



IRA WINKLER and DR. TRACY CELAYA BROWN

YOU CAN

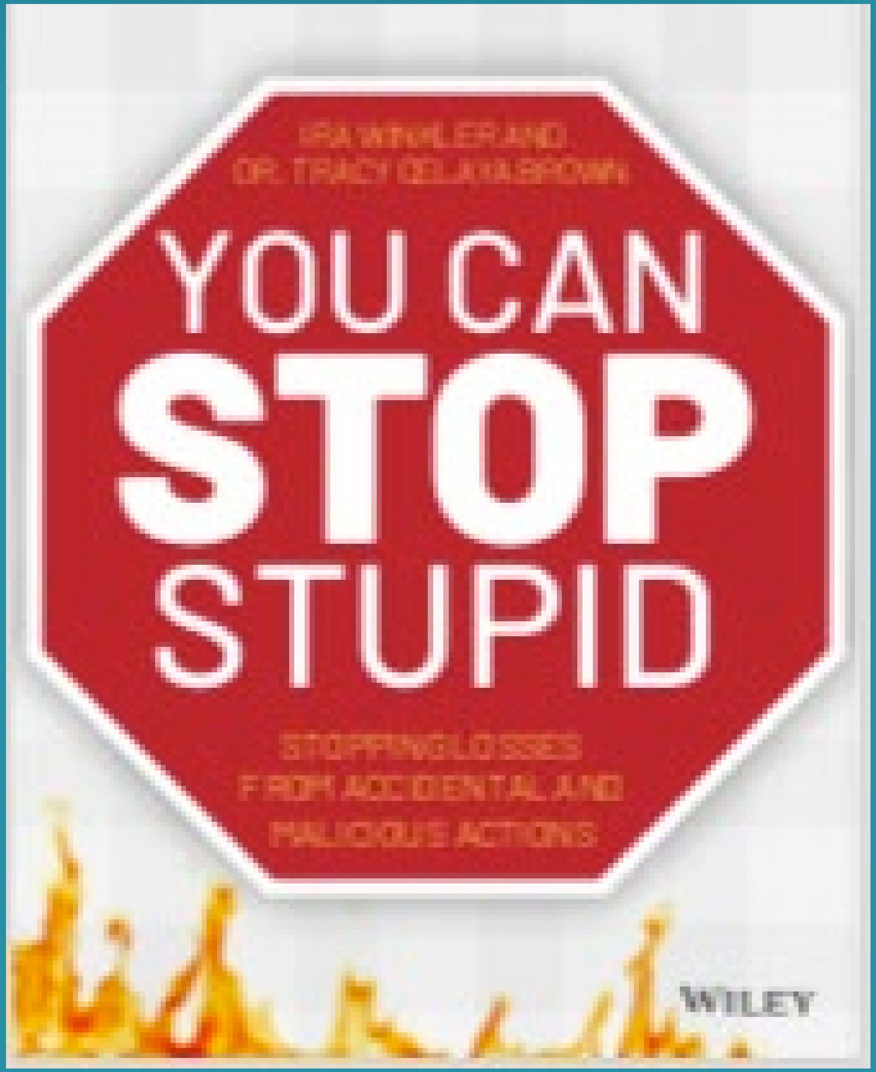
STOPPING LOSSES FROM

STOP

ACCIDENTAL AND MALICIOUS ACTIONS

STUPID

WILEY



IRA WINKLER AND
DR. TRACY CELAYA BROWN

YOU CAN
STOP
STUPID

STOPPING LOSSES
FROM ACCIDENTAL AND
MALICIOUS ACTIONS

WILEY

For More Information

ira@trustwave.com

+1-443-603-0200

www.facebook.com/ira.winkler

@irawinkler

www.linkedin.com/in/irawinkler

tracy@startwithgo.com

+1-480-559-0744

https://www.facebook.com/DrTreCB

@DrTreCB

www.linkedin.com/in/tracycelaya/

Trustwave