

Incorporating Security Practices Into Business Processes



Ira Winkler, CISSP
ira@securementem.com
+1-443-603-0200

Dr. Tracy Celaya, CISSP
tracy@startwithgo.com

Dr. Tre



I Cube

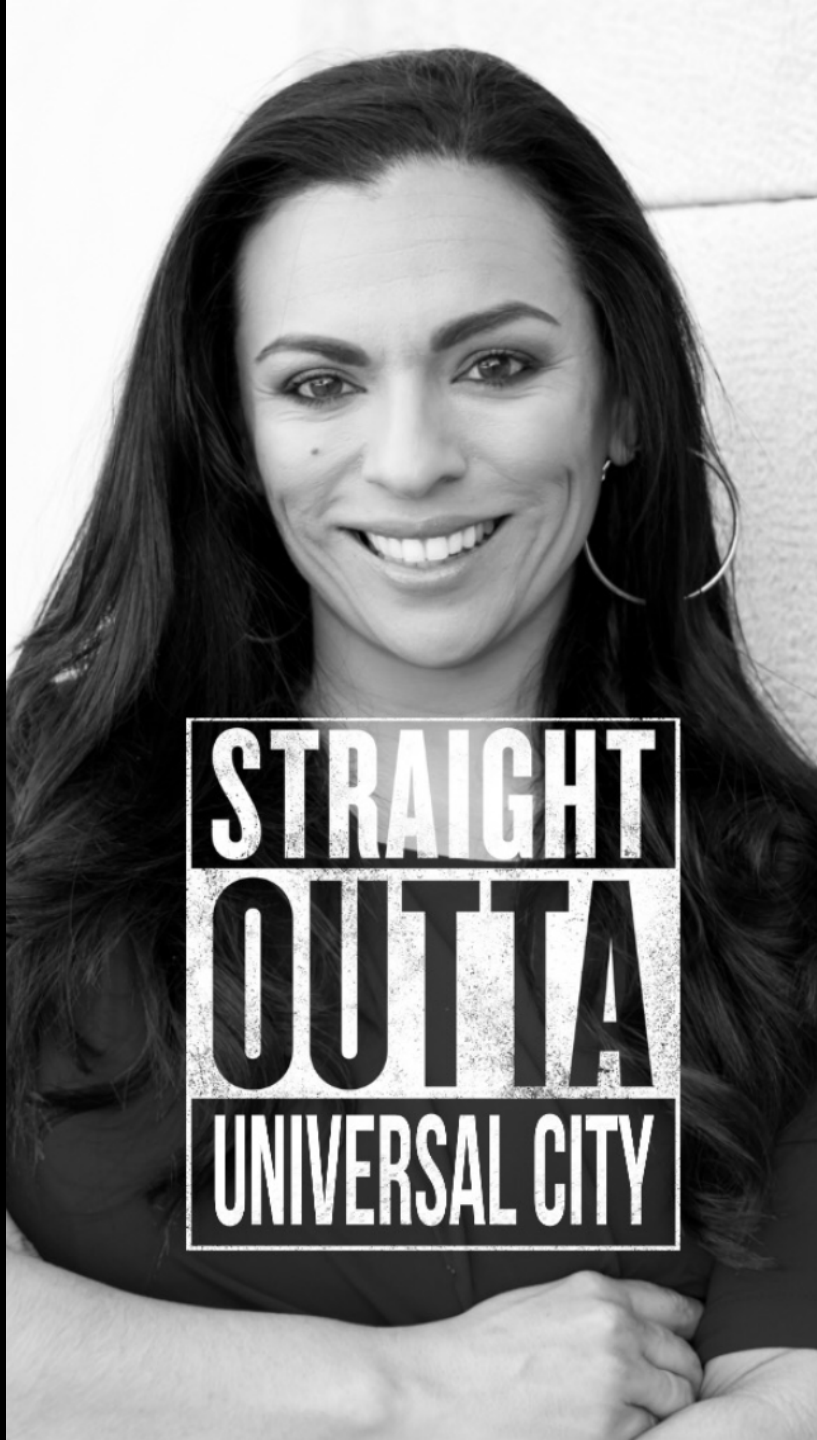


Hakkaz Wit Attitudes

#HakkazWitAttitudes

H.W.A

#HWA



**STRAIGHT
OUTTA
UNIVERSAL CITY**

#DrTreGonnalceIceCube

#IceCube

SECURE
MENTEM



A Couple Warnings

- You might disagree with us
 - That's ok, as long as it gets you thinking
- Each section of this presentation can be a separate presentation
- This is about getting you thinking and getting you motivated to take action
- Awareness is used as an example, but is not the only application of this content
- You should want to reevaluate your awareness methodology

SECURE
MENTEM

Why Do You Drive Safely?



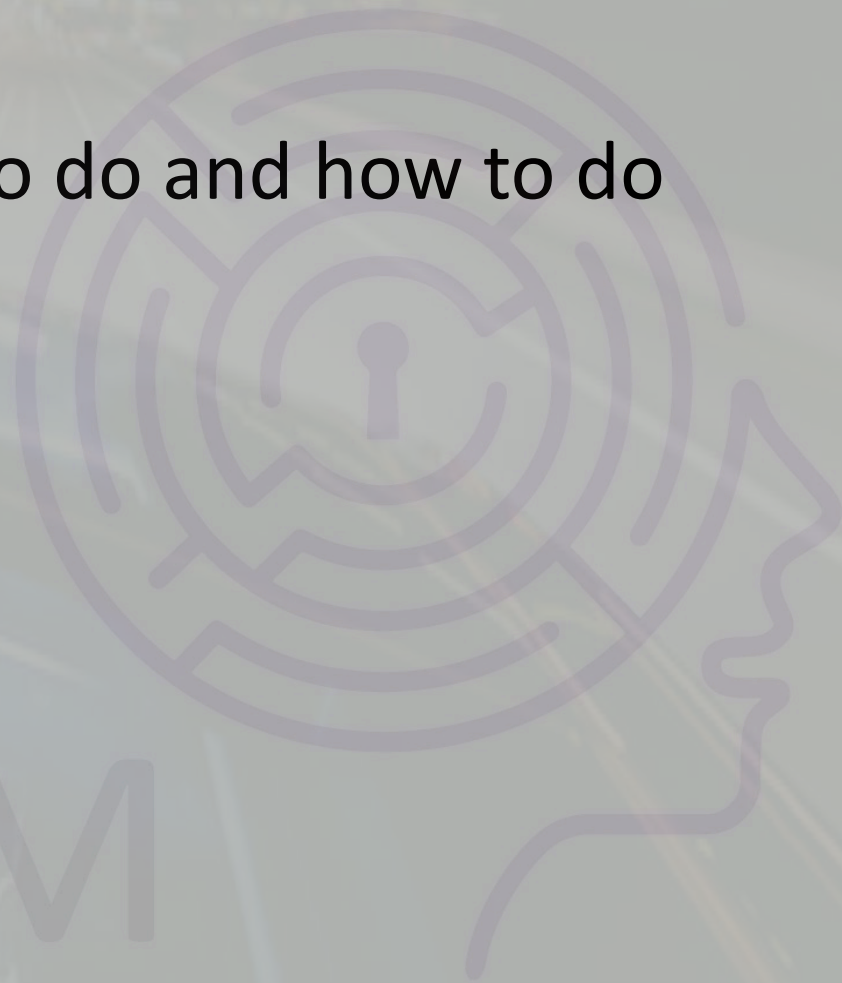
- Isn't it easy to drive dangerously?
- Isn't it less convenient to drive safely?
- How frequently do you take mandatory training?
- Why do you drive safely?
- Why wear seatbelts?

MENTEM

Why Did You Not Get Killed On Your Way Here?

- How frequently do you take mandatory safe pedestrian training?
- Why do you know what to do and how to do it?

SECURE
MENTEM



Shower in the Dark

- You know where everything is
- You have a process
- It's autopilot



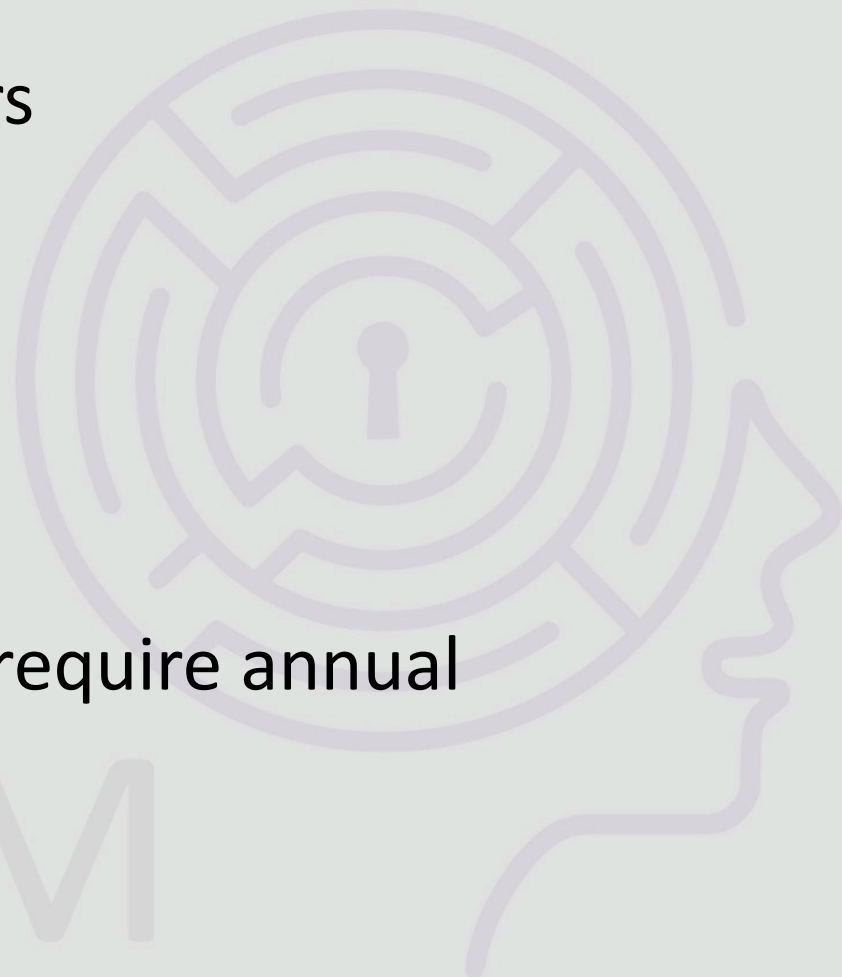
SECURE
MENTEN

In The Workplace

- How many things do you do, because you know to do it?
- Not face-planting into doors
 - Unless you work at Apple
- Submit hours worked
- Your daily functions
- Wear badges
- Not watch porn
- How many of these things require annual training?



SECURE
MENTEM



Humans Like Consistency

- It's a fundamental human need
- Homeostasis
- Resistance to change
- Routes taken to work
- Grocery stores
- Coffee Shops



SECURE
MENTEM

Important = Procedure or Guideline

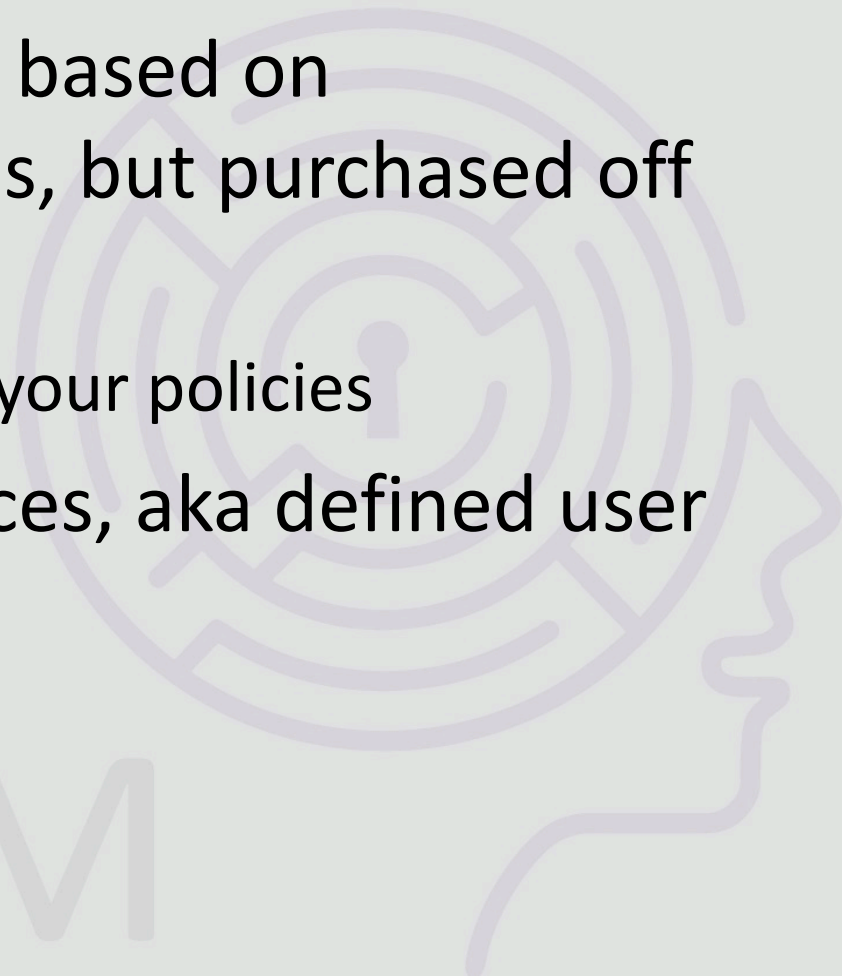
- Processing of financial documents
- Onboarding of personnel
- Auditing of business processes



It's Not the Same with Security

- User behaviors are poorly defined
- Awareness training is not based on procedures and guidelines, but purchased off the shelf from vendors
 - You're letting vendors set your policies
- Rarely are security practices, aka defined user actions, documented

SECURE
MENTEM



Shoulds versus Musts

- If something is a Should, it gets done if all else is good
- If something is a Must, it will get done
- Most companies should all over themselves
- Are security behaviors for you a Should or a Must?

SECURE
MENTEM

Awareness Programs Should All Over People



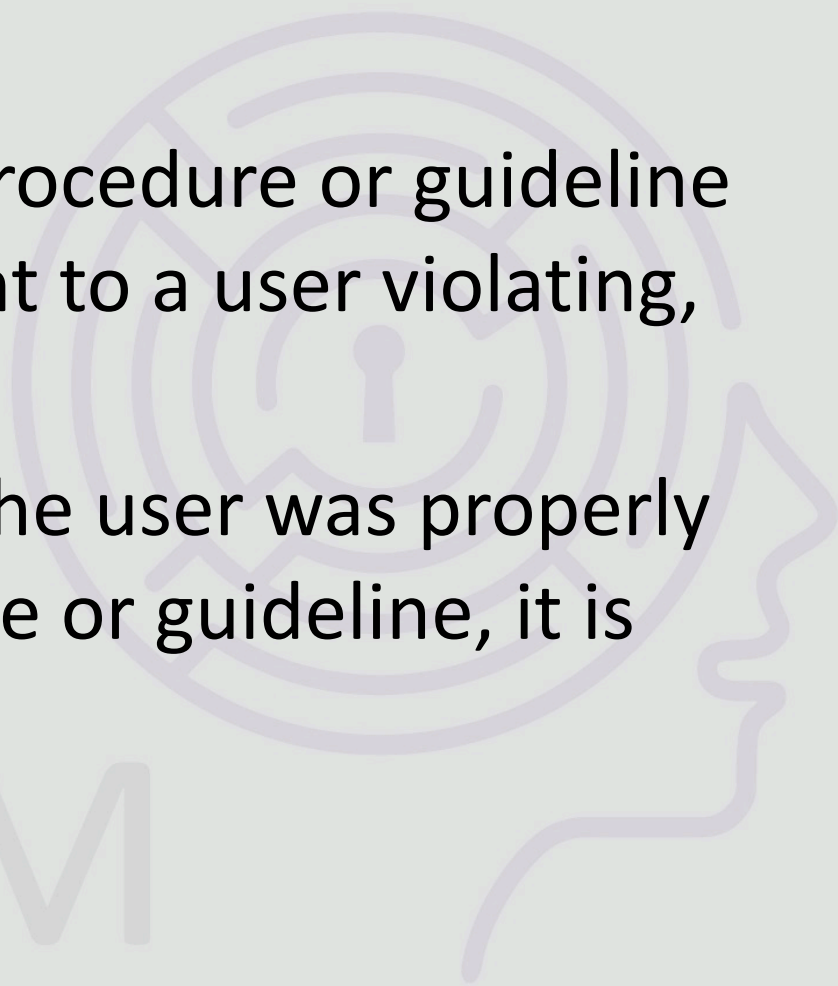
SECRET
MENTALITY



Behind Every Stupid User...

- ...is a stupider security professional
 - Usually
- If there is not a specific procedure or guideline in place that you can point to a user violating, it is your fault
- If you cannot show that the user was properly informed of the procedure or guideline, it is your fault

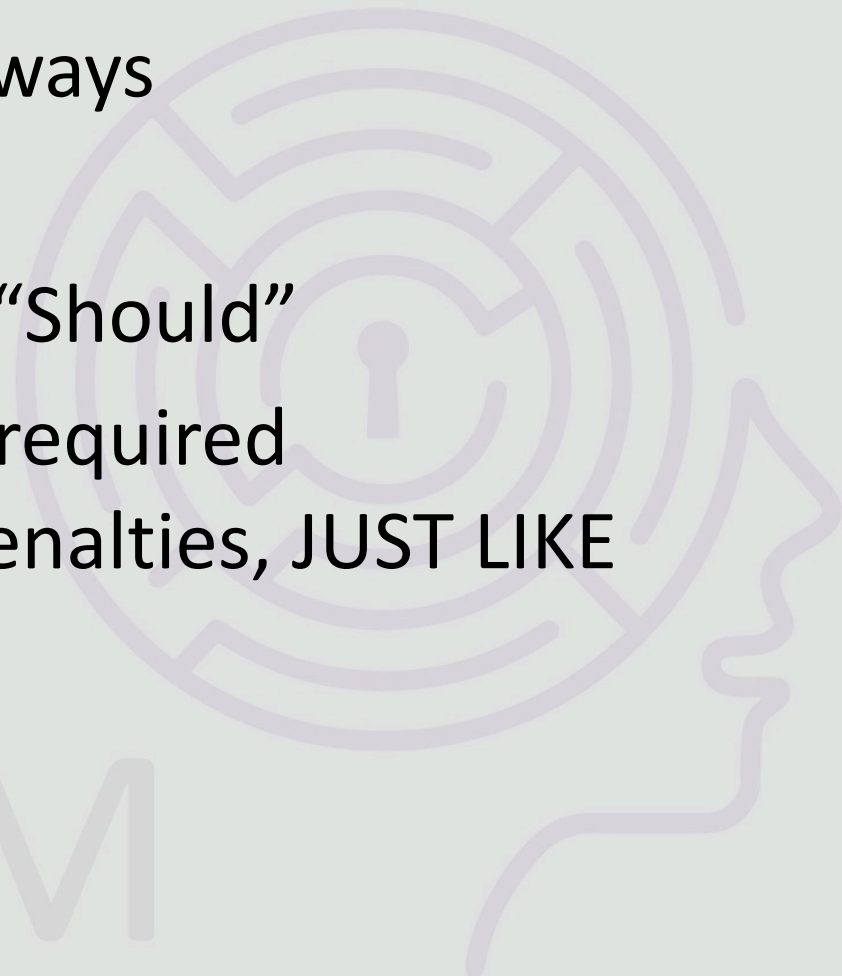
SECURE
MENTEM

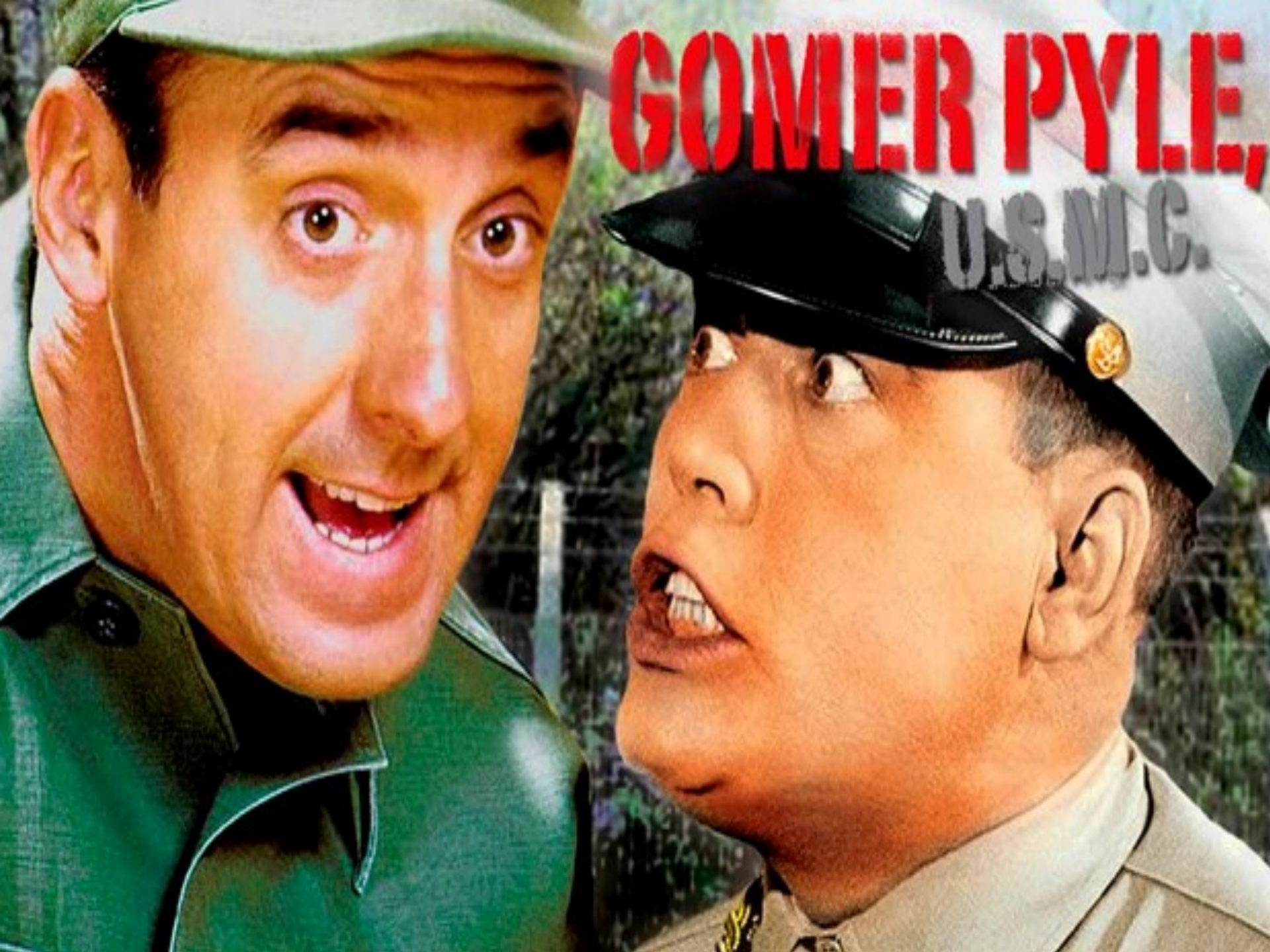


Most Awareness Programs Are Just Gimmicks

- They choose entertaining videos
- They come up with giveaways
- Tests of finite knowledge
- They treat security like a “Should”
- They are afraid to define required behaviors/actions with penalties, **JUST LIKE ANY OTHER POLICY**

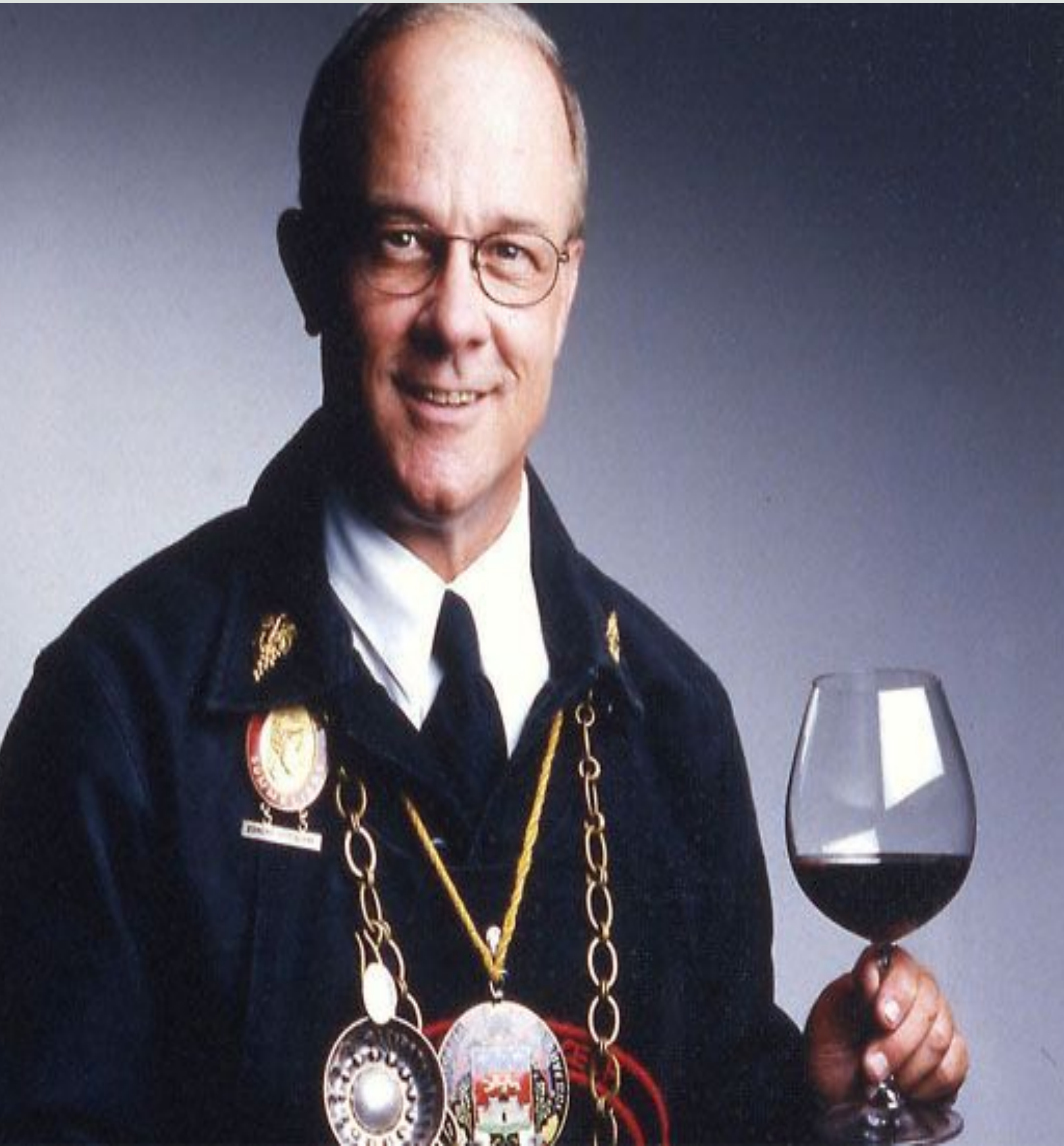
SECURE
MENTEM





GOMER PYLE, U.S.M.C.

Sommelier vs. Grandma



DETERMINING BUSINESS PROCESSES TO ADDRESS

SECURE
MENTEM

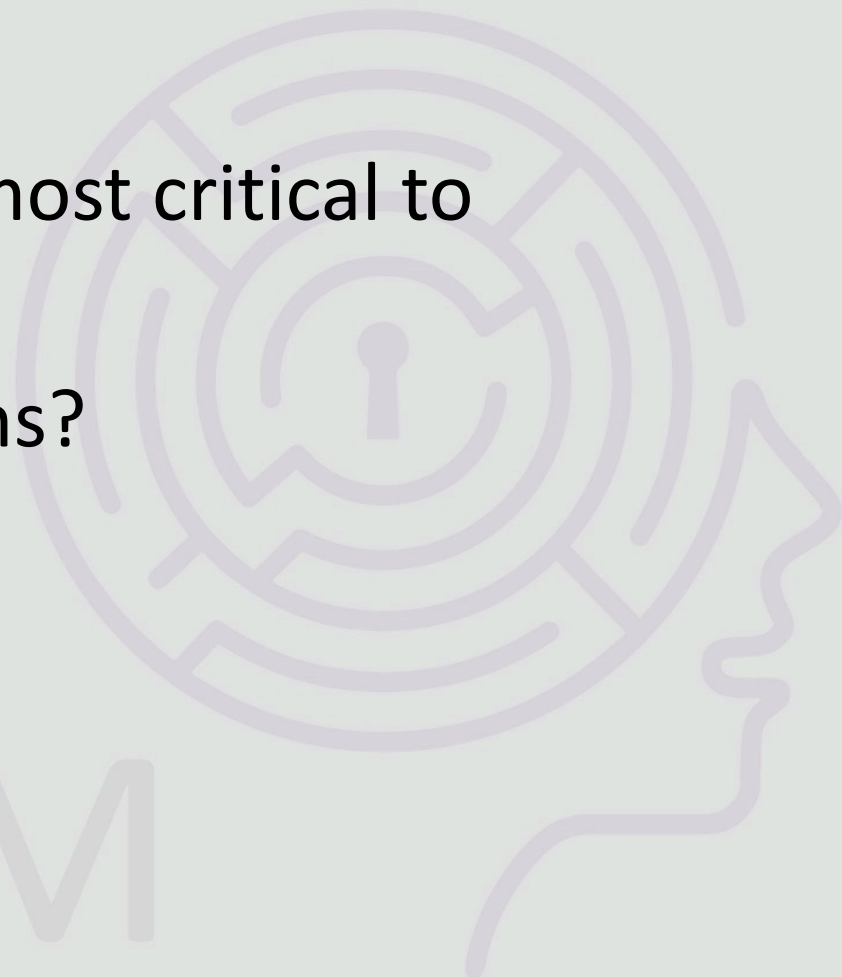


Countless Processes to Address

- You have to start somewhere
- Need to prioritize
- What processes are the most critical to business operations?
- Where are there easy wins?



SECURE
MENTEM



Try to Get C-Level Support

- Ask CEO, CIO, CFO, etc for important processes
- Ask them for connections
- Ask for support
- Ask for their help



SECURE
MENTEM



Past Incidents

- What processes were involved with significant incidents
- What processes were luckily missed in significant incidents
- Changes implemented after incidents



SECURE
MENTEM

Critical Processes

- Financial processes
- Failures that result in significant financial loss
 - What is the definition of “significant financial loss”
- Directly affect the business’ ability to continue
- Must be restored immediately after a disruption to ensure business continuity
- Satisfy regulatory compliance



SECURE
MENTEM

Easy Wins

- What business areas are amenable to security enhancements?
- Where are your best connections?
- New processes
- Processes being modified
- Processes being automated
- Send out broad solicitations



SECURE
MENTEM



What Are They Doing?



- Handling Data/Information
 - Intellectual Property
 - Customer & Employee Data
 - Trade Secrets
- Responsible for Securing Devices
- Financial Transactions
- Vendors and Third-Party Suppliers
- Compliance & Regulations
- Accessing the Network
 - Emails
 - Internet
- Social Media
- Traveling
- Talking to Strangers
- Potential Internal Threats

SECURE
MENTEM

Prioritization

- Again, you want to look at all processes
- Start with most critical processes
- Make sure you can get in easy wins
 - You need to market wins



PRIORITIES

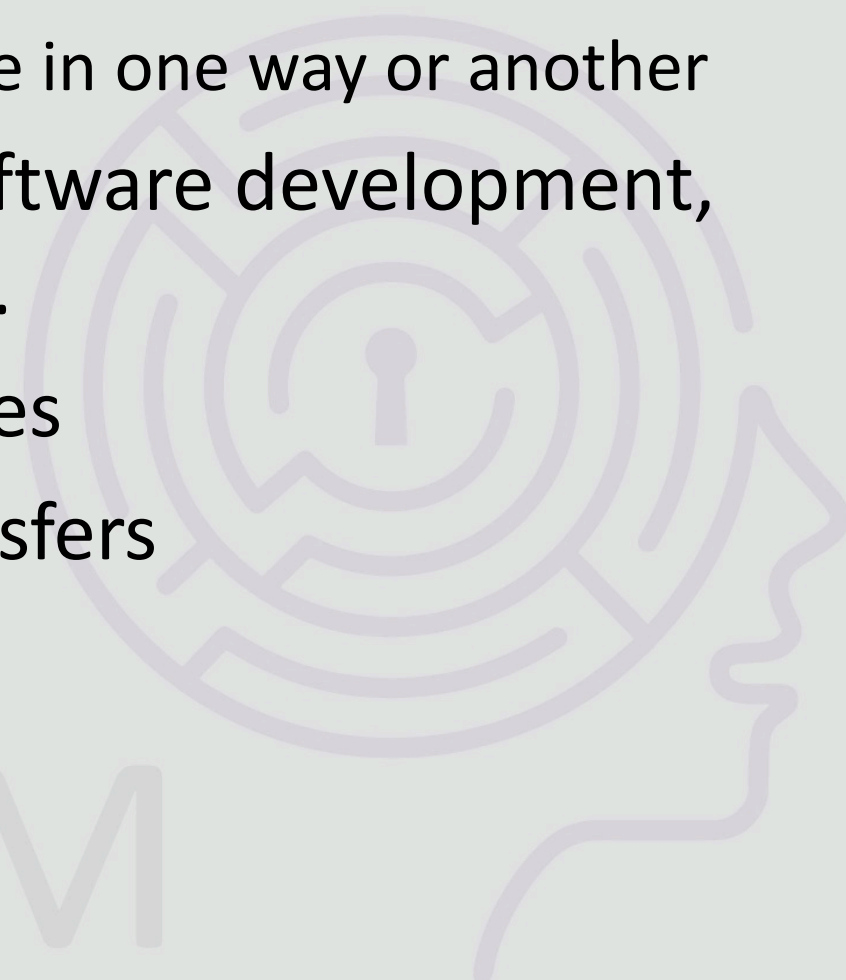
- 1.
- 2.
- 3.

SECURE
MENTEM

It's Not Just People We're Concerned About

- Well, kind of
 - Everything involves people in one way or another
- Security embedded in software development, system maintenance, etc.
- Supply chain related issues
- Automated financial transfers
- Etc

SECURE
MENTEM



EMBEDDING SECURITY PRACTICES

SECURE
MENTEM



Where Can Security be Added



- ...or where is it lacking?
- Need to understand the underlying processes
- Analyze every step for potential vulnerability
- Find out if there's a backstory
 - There might be a reason things are they way they are
 - Don't ignore those lessons
 - You don't have to leave them alone, but you need to account for them

SECURITY
MENTEM

For Each Step of a Process:

- Is there a decision point?
- Is that decision point defined?
- Is there room for discretion?
- Could be for people or technology
- Yes, you are minimizing user discretion

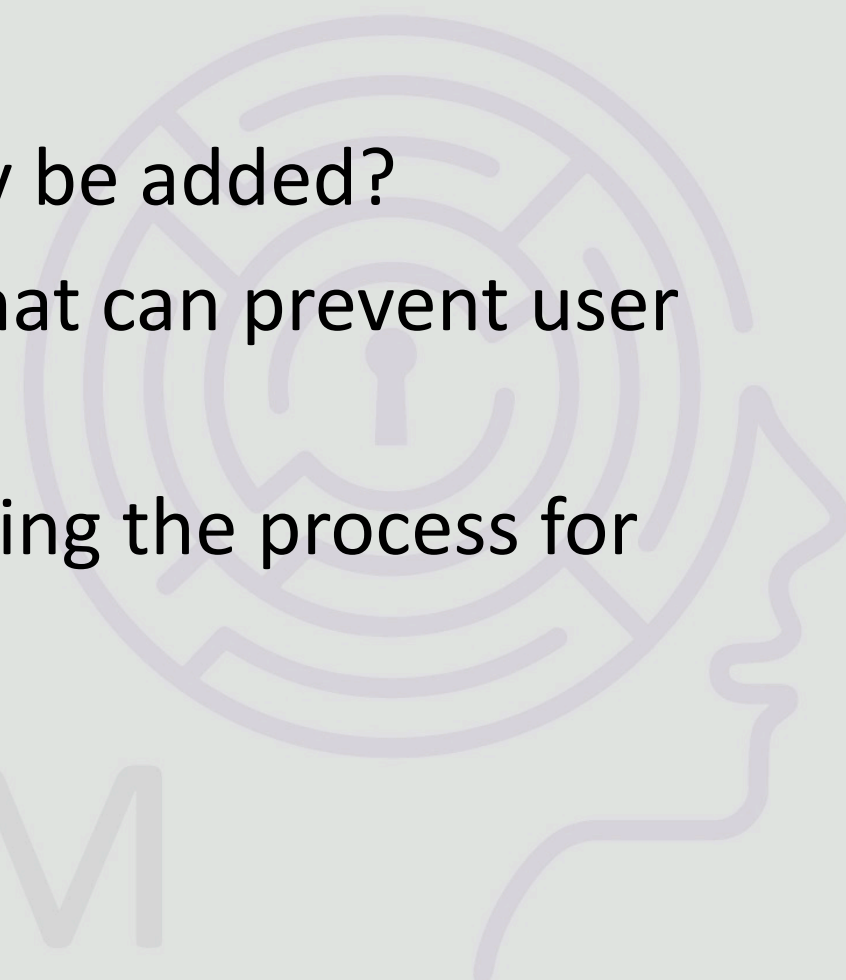
If a user causes harm, if there is no procedure or guideline specifying a different action, it's your fault

SECURE
MENTEM

Even Without People

- Is security apparently considered as part of the process?
- At each step, can security be added?
- Are there technologies that can prevent user actions/mistakes?
- Yes, you are micro analyzing the process for security considerations

SECURE
MENTEM



Learning From Incidents – R.I.F.



Review past critical incidents

Identify root causes

Fill in the procedural gaps
with security in mind

Building in Exception Handling

- There will be required exceptions
- Handling exceptions must be well defined
- Attackers will attempt to create exception handling
- Developers on tight schedules might need exceptions
- Critical outages might require exceptions

A graphic illustration of a hand holding a sign. The hand is black with white outlines, and the sign is green with white text. The background is a light brown color. The text on the sign reads "THE EXCEPTION".

THE
EXCEPTION

PROVES
THE RULE

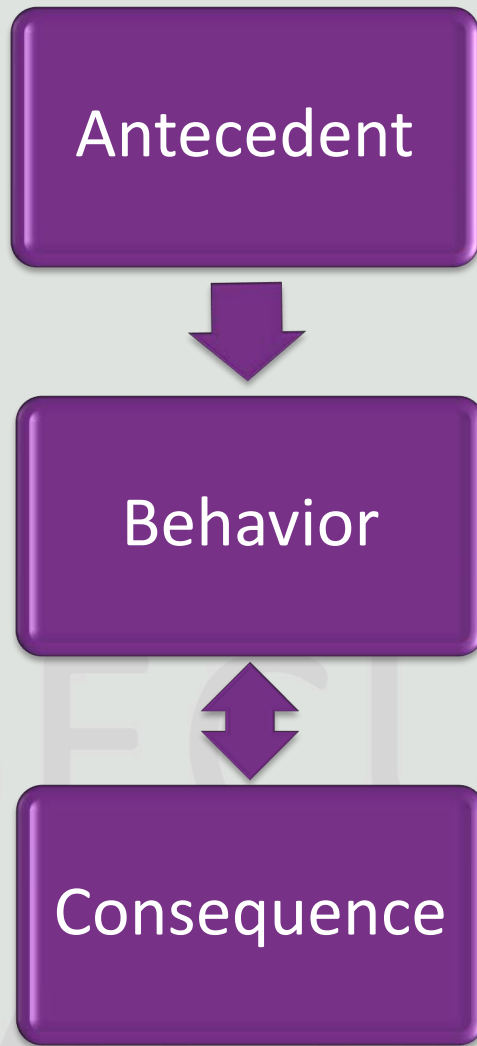
Implementing awareness



- Becoming Grandma



ABCs of Behavioral Science

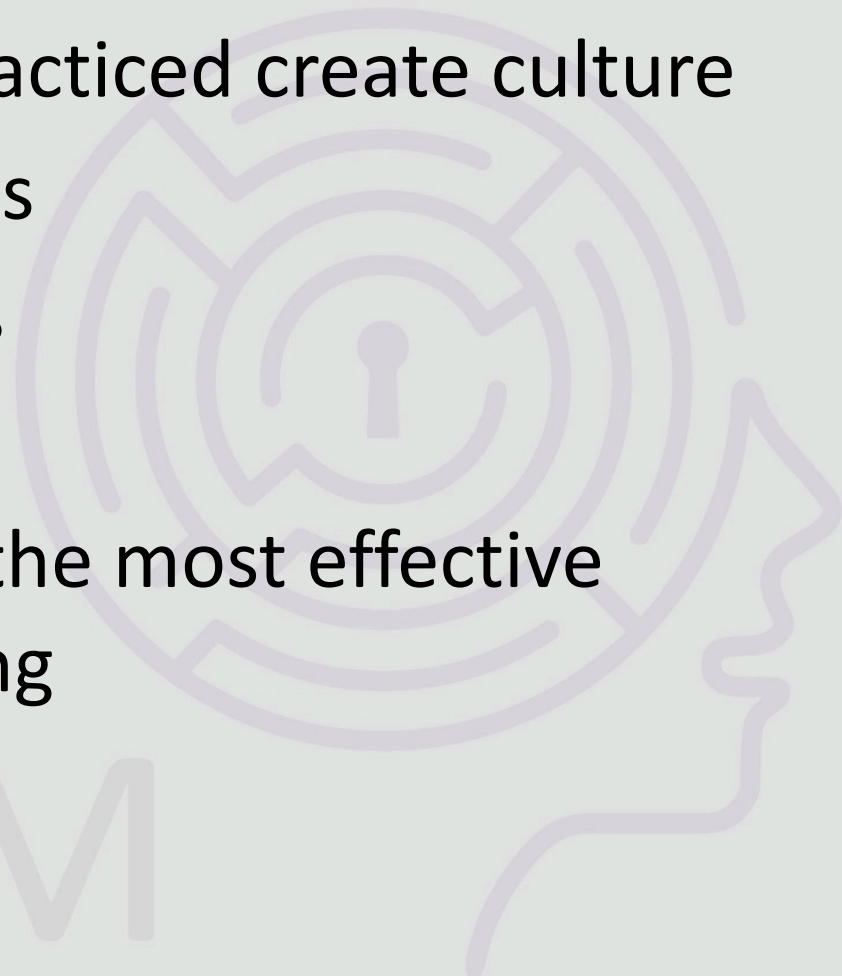


- Antecedent might create up to 20% of behaviors
- Consequences create 80%+ of possible behaviors
- Consequences can be positive, negative, or neutral
- Positive consequences can reinforce bad behaviors and vice versa

ABCs of Awareness

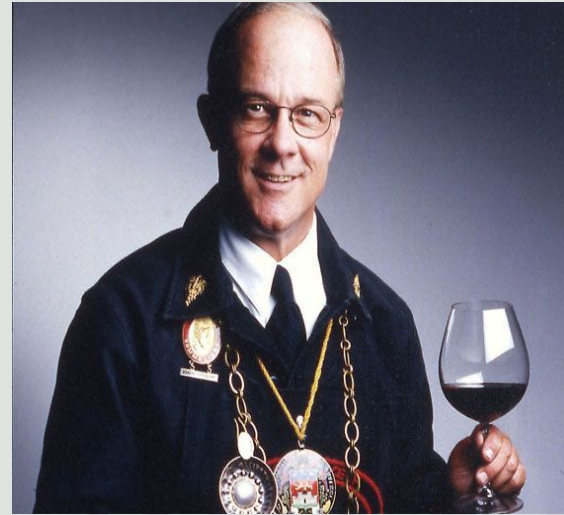
- Awareness creates behaviors
- Behaviors consistently practiced create culture
- Culture creates awareness
- Culture creates behaviors
- Culture is peer pressure
- Peer pressure should be the most effective form of awareness training

SECURE
MENTEM



In Other Words

Awareness =



Culture =



SECURE
MENTEN

Motivation, NOT Entertainment

- Awareness has 3 parts
 - Information about the problem
 - Solution to the problem
 - MOST IMPORTANT, motivation to implement the solution
- Funny ≠ Motivation
- Your goal is to impact behaviors, not provide chuckles
- Motivation can be fun, but...
- ...Awareness efforts lose sight of the goal of changing behaviors



Institutionalizing Peer Pressure

- People need to do it, because they need to do it
 - Like. Every. Other. Process. In. The. Organization.
- Specifying expectations in detail
- Everyone must know the details
- Everyone must become responsible



Musts Are Good

ALL EMPLOYEES MUST:

1. Tape Webcam
2. Tape Microphones
3. Install Password Manager
4. Enable 2FA on their accounts
5. Use a Hardware Token

Do **NOT** use Hooli products.

Do **NOT** post pictures or videos of the office
on Social Media.



Creating a Culture is a Presentation Itself

- This isn't about awareness
- It's about creating a culture – NOT UNDERSTANDING IT
- You're creating MUSTS
 - Instead of shoulding all over people
- That's your job as a security manager
- Gamification to implement
- Frankly, negative consequences are mostly required
 - It's expected to do things right
- Exception handling must be drilled into people



SECURITY
MENTEM

Final Analogy

- With financial crimes
 - They don't make ruining the company a joke
 - They don't say, "You're an accountant. Maintain the books, and by the way, some people might try to steal money. Watch out for that."
 - They create good procedures that prevent and detect the crimes proactively

Why don't organizations do this with cybersecurity?

Process, Not Fear

SECURITY
MENTEM

Most Important

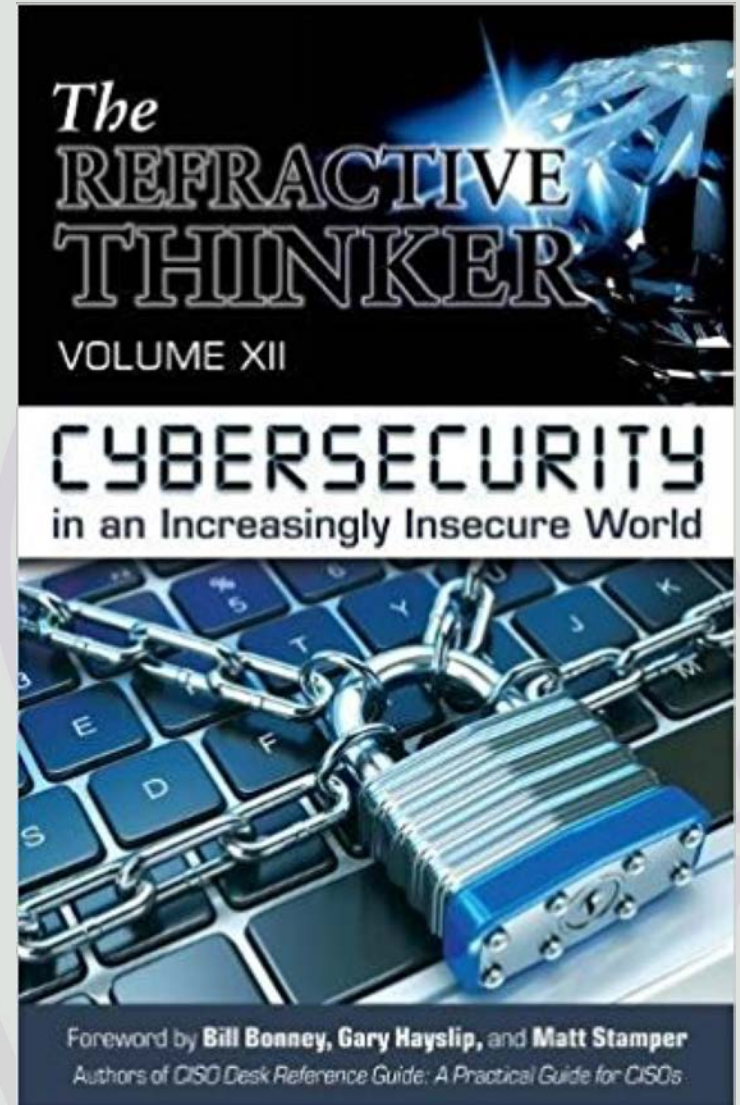
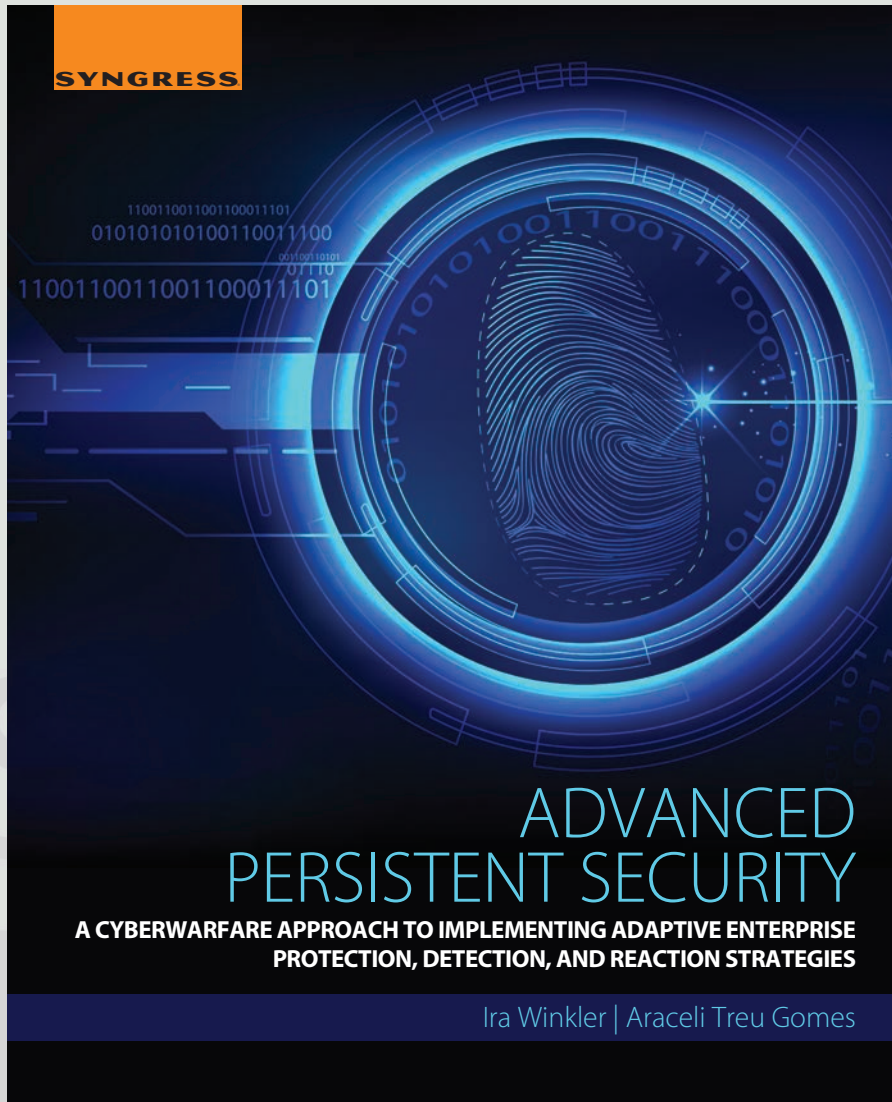
What are your thoughts about this?

Rhetorically, but if you have questions, ask them
in 2 minutes

SECURE
MENTEM



The Books, The Myths, The Legends



For More Information

ira@securementem.com

+1-443-603-0200

[@irawinkler](https://www.linkedin.com/company/irawinkler)

www.securementem.com

www.linkedin.com/in/irawinkler

[Facebook.com/irawinkler](https://www.facebook.com/irawinkler)

tracy@startwithgo.com

@_tracycelaya

www.startwithgo.com

SECURE
MENTEM

