# RSA Conference 2019
## Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

BETTER.

# 30+ Years of Security Awareness Efforts:

# What have we learned?

**Ira Winkler, CISSP**

President, Secure Mentem
Advisor, HoxHunt
@irawinkler

#RSAC

# Seminal Hasn't Changed Much...Sigh

## 1995 USENIX UNIX Security Symposium

- Do not rely upon common internal identifiers

- Implement call-back procedure for information disclosure

- Implement security awareness program

- Identify direct computer support

- Create a security alert system

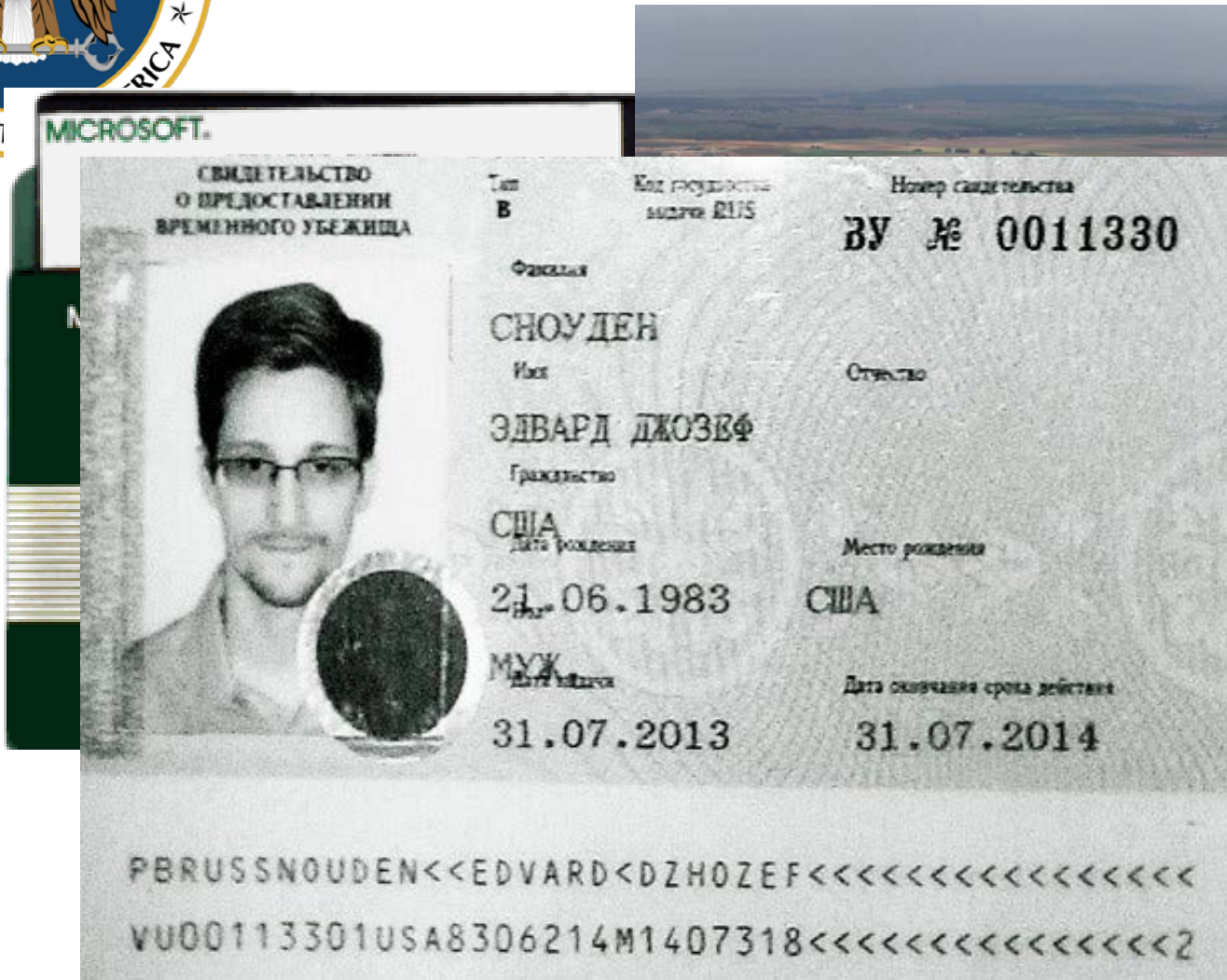- Perform social engineering to test security

## 2018 Social Engineering Webinar

- Be paranoid

- Train client facing staff

- Verify identity with other information

- Implement MFA

HOXHUNT

RSA Conference2019
Asia Pacific & Japan

# The Bad Awareness

# The Good



- There are some really screwed up people there
- Despite a couple disasters, there are relatively few significant security problems
- People do accept security procedures when expected to

# Social Engineering Doesn't Qualify You as an Awareness Expert

- I know first hand

- Social Engineering is easy
  - Amateurs are easily successful

- Social engineering can determine unique problems, and possibly the scope

- Awareness is more than telling people, "Here are problems; Don't fall for that!"

- Knowing how to break something does NOT mean you know how to fix it
  - It's a completely different science

# Corollary: An NLP Course is Not a Substitute for Real Human Elicitation Training

- Good spies seem to have a 6$^{th}$ Sense
- Their lives depend on it
- Intelligence operatives have years of training
- NLP is good background, but not the same
  - Maybe it's usually enough
  - 90% successful with just the nerve
- Give up a password vs Betray country under penalty of torture and death

# Yes, You Can Patch Stupid

- You better expect users to make mistakes

- Patching is not getting rid of a problem, but implementing a protection

- More later, but…
  - You can prevent attacks from getting to the user
  - Taking decisions away from users
  - Proactively mitigating attacks after the fact

# You, NOT the Users, Are the Weakest Link
## (Behind Every Stupid User is a Stupider Security Professional)
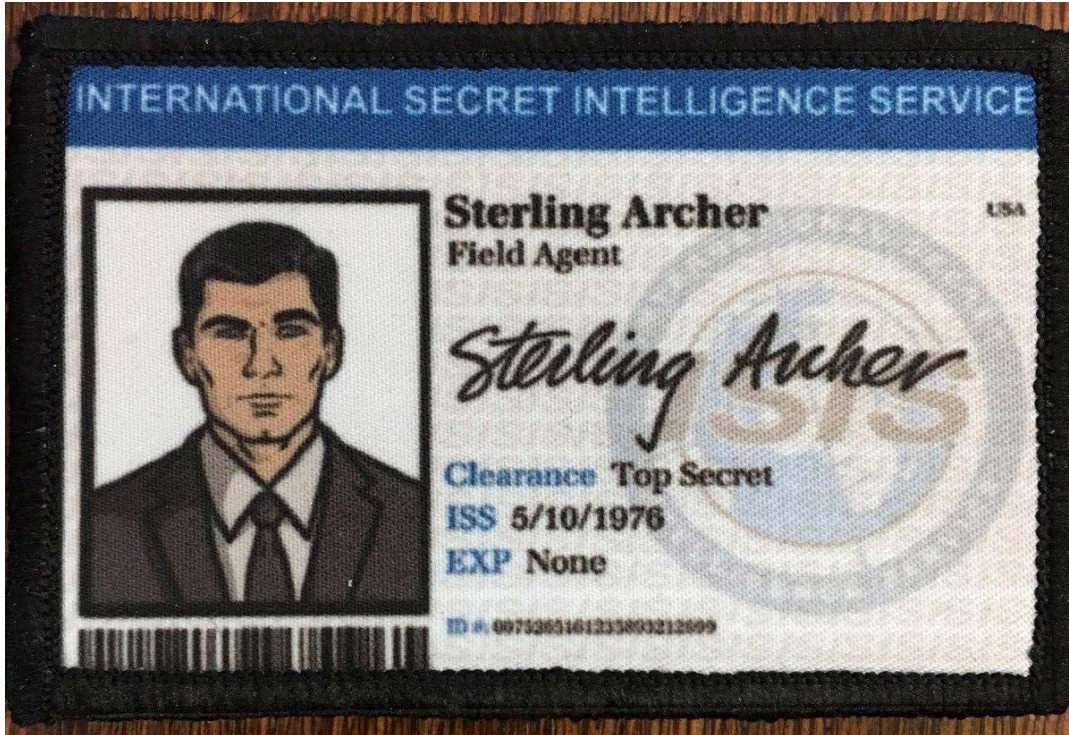
- Users are a part of the system you are there to protect

- If you can't secure a critical part of the system, it's your fault

- Calling the user the weakest link abdicates responsibility

- If the user can ruin your network, IT'S YOUR FAULT!

INTERNATIONAL SECRET INTELLIGENCE SERVICE

**Sterling Archer**
Field Agent

USA

Clearance Top Secret
ISS 5/10/1976
EXP None

**HOXHUNT**

RSAConference2019
Asia Pacific & Japan

# Users Are NOT the First Line of Defense



Such a truck would be good for picking up girls in Minsk.

- Grandiose terms about users are as bad as disparaging terms
- The users are part of the system
  - They are not a resource to the security team
- They are not the first line of defense
  - You facilitate the attacks getting to them
- They are really not a reliable line of defense

# The Human Firewall Isn't

- In the first place, technical firewalls fail miserably

- In the second place, just don't

- A human firewall is even more unreliable than a real one

- Users are again not your resource

- Humans are a part of your system

# Yes, You Can Blame the User

- Well, as long as the user should know what to do
  - You need a "Just Culture"

- Not following policies and ruining the network/organization should be punished
  - It is literally done with every other business function in an organization
  - Remember the NSA contractors who gave Snowden their passwords

- When you have no enforcement, you have no security program

# Stop. Think. Connect. Just. Don't. Do. It.
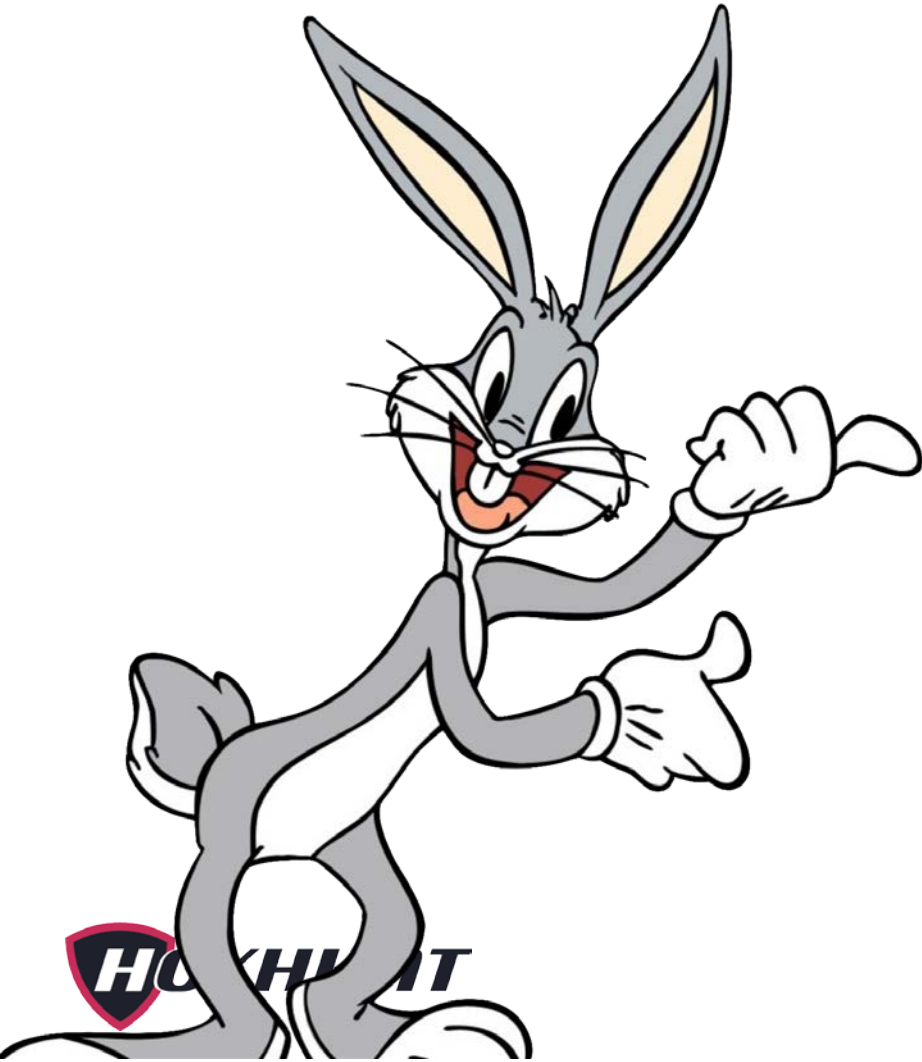
- STC is a popular campaign

- Novices vs Skilled Sociopaths

- It's a losing equation

- Training people to be on the lookout for the Wascally Wabbit

# Gamification Does NOT Mean a Game…

# Funny ≠ Effective

# Some Examples

- You lose your weapon, you will do jail!

- You lose your badge, you have to pay $100 for a replacement
  - It costs RSA money
  - It prevents badge duplicate badge use

- You don't badge in, you don't get paid

- You email out PII, you will be called into the office
  - Laws require it now
  - It costs companies money

# Sommelier Vs Grandma
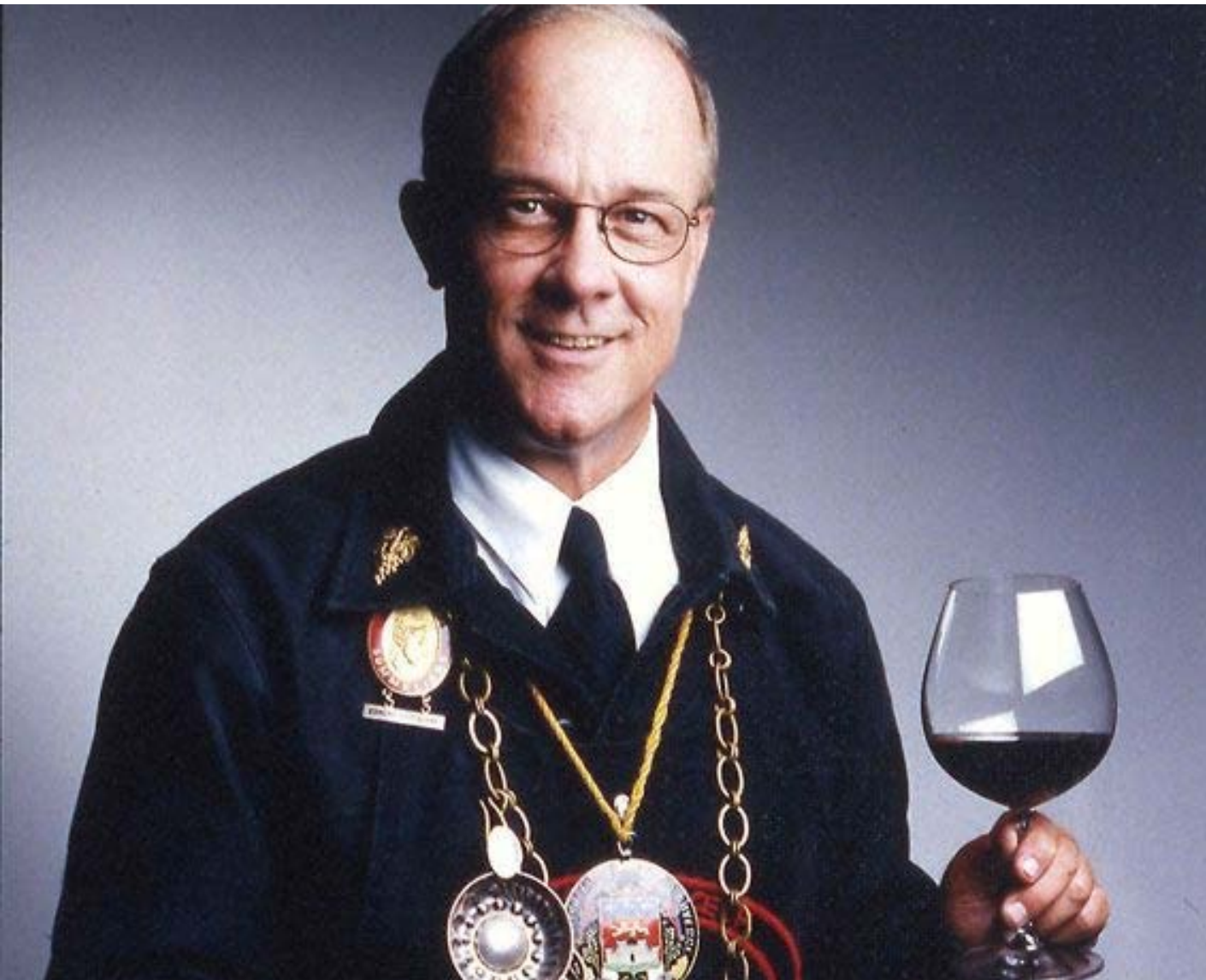
# Awareness Programs Should All Over People

# Likability is NOT a Valid Awareness Metric

- Whether or not people like your training is not a valid measure of effectiveness

- There must be motivation to practice the desired behaviors

- It doesn't matter if people know why they're doing something

- It doesn't matter if it's funny

- They just have to do it

*Does it change the behavior?*

# RSA®Conference2019
## Asia Pacific & Japan

# Why Awareness?

# Awareness is a Business Function

- Awareness is there to reduce business losses

- If it's just a Check the Box, it doesn't matter
  - You might as well do anything

- The only thing that matters is that you return more investment than the cost of the awareness program

ONE DOES NOT SIMPLY

CHECK THE BOX, OR MAYBE THEY DO

# RSA®Conference2019
## Asia Pacific & Japan

**Security efforts get the budgets they deserve, not the budgets that they need**

*Learn to deserve more!*

# Psychology

- I realize it's counterintuitive

- Psychology is the study of the individual

- Individuals are mostly different

- You can't have a different awareness program for every person

- It helps, but it is too fluffy

# Mental Models Don't Help

- How someone perceives something and makes a decision

- Some studies indicate Mental Models don't help with security

- One study showed that the wrong Mental Model can be the best
  - It doesn't matter what they know, it matters what they do

- Either way, your goal is to create the behavior no matter how each and every person in the company thinks

# ABCs of Applied Behavioral Science

Antecedent

↓

Behavior

↕
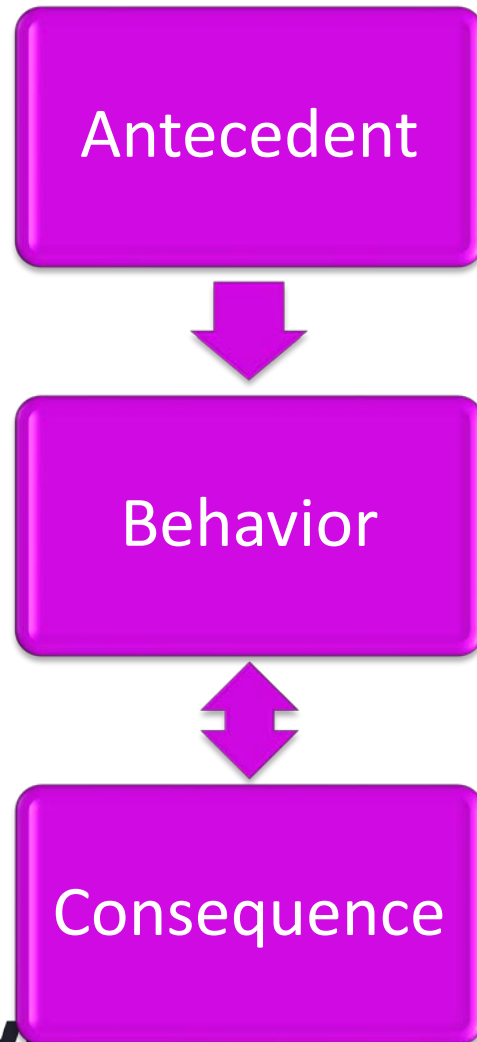
Consequence

- 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

# Gamification

- When implemented properly

- A reward structure for exhibiting desired behaviors

- For the right environments and roles

- Tactically for specific behaviors

- Business drivers tell you what to reward

- Culture tells you how to reward

# Safety Science

- Would you blame the canary in the coalmine for dying?

- Critical financial motivation
  - Injuries cost a lot of money

- 90% injuries from environment

- 10% from carelessness or ignorance
  - Assuming they know the appropriate behavior

- The last 10% is where awareness comes in

# Just About Every Other Business Function

- The CFO would be fired for saying people-related losses are too hard to control

- The COO would be fired for saying that they can't get the employees to do their jobs properly

- McDonald's automates away just about every employee decision

# It's More than Phishing and CBT

- Pervasive

- You are creating a culture

- Any communication tool that will work
  - Speakers
  - Newsletters
  - Coffee cup sleeves
  - Anything

# The Components of an Awareness Program

- Topics driven by business drivers

- Communications tools driven by culture

- Metrics driven by
  - Business drivers to measure what's important
  - Culture to determine what is easy and available to measure

# About Metrics

- Should measure the root behavior
  - Not the symptoms
  - Reports of phishing messages
  - Anti-malware reports
  - Calls to the Help Desk
  - Stopping strangers

- Should be real business practices

# Culture is the Best Awareness Tool

- When everyone does the right thing everyone will do the right thing

- With our without an awareness program, everyone does what everyone else does

# Address Security Like Every Other Business Process

- Remove decision making process from users

- Governance to determine process specifically

- Technology to implement process
  - Eliminate decisions where possible (passwords, MFA)

- Governance defines behavior
  - Specifies how decisions are to be made

- Exception handling

# Which One Are You Creating?

**RSA**Conference2019
**Asia Pacific & Japan**

# The Big Question

## What Are You Trying To Accomplish?

## An Aware User or Mitigating User Related Losses?

# Awareness is Valuable, But…

- Generally 1 in 20 users will fail
  - That's 50 people for every 1,000

- All it takes is 1

- Risk reduction is critical though
  - Is it better to have 5 in 20 fail?

# …You Need to Reduce Need for Awareness

- Take away need for user action

- Take away the need to Think.

- Define decisions

- Force decisions

#RSAC

# **Apply**

- Within a week
  - Determine what type of awareness you have
  - Determine if you want to change it

- Within 30 days
  - Determine a plan to start migrating
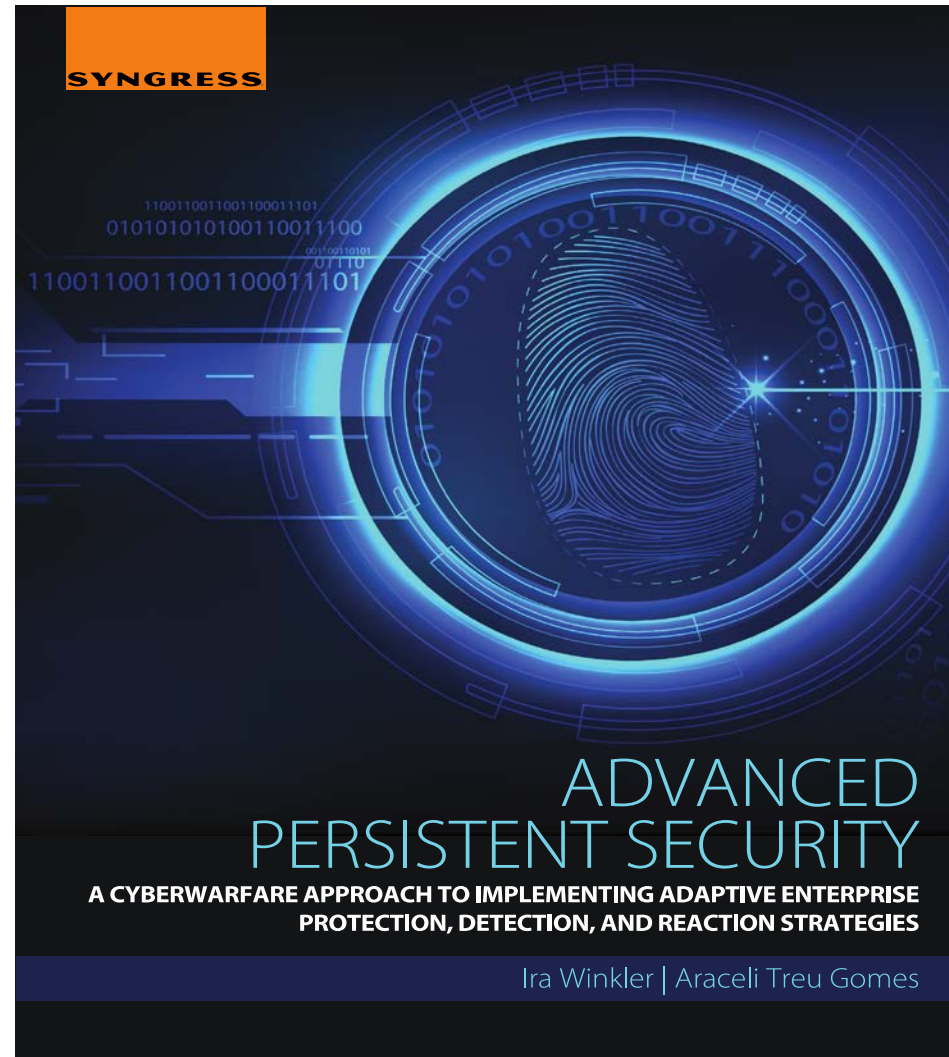  - Get support to implement plan

Within a 90 days

Create a plan

Determine first project to enhance awareness or human security

Implement low hanging fruit

Buy my book

RSAConference2019
Asia Pacific & Japan

# The Book, The Myth, The Legend

# The Next Legend

# You Can Stop 'Stupid'

@CanStopStupid

HOXHUNT

RSAConference2019
Asia Pacific & Japan

# For More Information

@irawinkler

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

www.securementem.com

+1-443-603-0200