RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: LAB1-W03

Holistically Mitigating Human Vulnerabilities & Attacks

Ira Winkler, CISSP
President
Secure Mentem
@irawinkler

Dr. Tracy A. Celaya, CISSP
Principal Consultant
Go Consulting Int'l
@DrTracyC

Alexandra Panaretos CSAP
EY Americas Lead Security Awareness
EY
@Cyber_Simple

Objectives

- Understand the human factor as a vulnerability
- How the Kill Chain is represented in human based attacks
- Holistically analyze human based attacks
- Apply countermeasures to the Kill Chain
- Understand how Ira can make enemies of Nation States and digitally lived to tell about it

The Problem

- The human is considered the weakest link
- Anytime a user fails, it is considered an awareness failing
- People then question the value of awareness
- Nothing changes

The Reality

- Successful attacks against users result from a systematic failure of the entire security infrastructure
- Technology, Governance, and Awareness address issues in silos without coordination
- Security teams seem literally afraid to do anything significant to change culture

Some Things to Think About

- If a user can ruin your network, your network sucks
- If your network sucks, your security team sucks

Awareness Isn’t Perfect

Most Awareness Programs Are Not

- Frequently limited to computer-based training (CBT)
- Not practical
- Always reliable; even phishing simulations don’t necessarily protect you from real phishing attacks
  - Frequently train people to recognize the simulations
- Focused; most awareness of other attacks is focused on specific situations

Even Smart People Make Mistakes

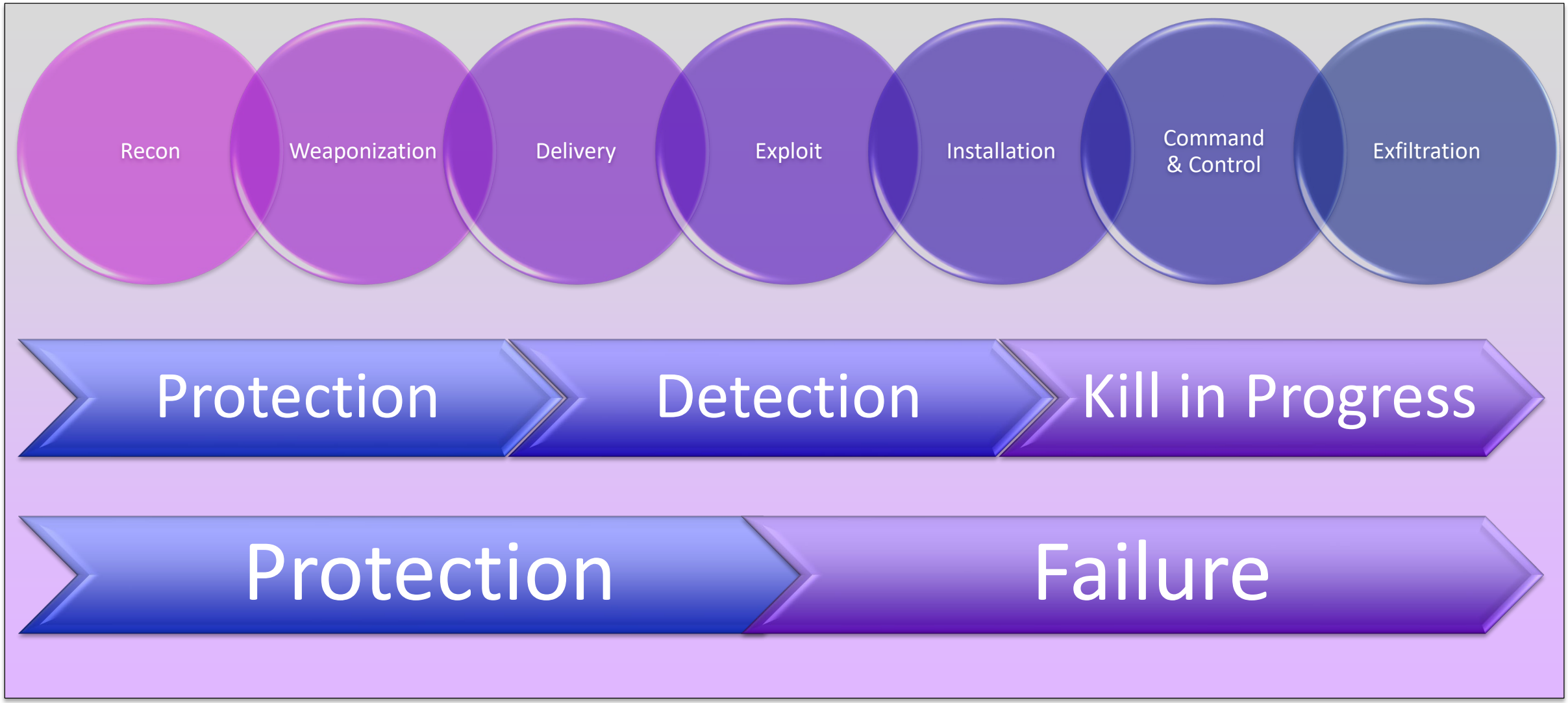
- How many of you have clicked on a phishing message?
- How many of you let visitors in doors, or posted too much on the Internet?
- How many of you remember all of your passwords, especially at work?
- Accidents happen
- Some attacks are very well crafted

Technology Failures

Kill Chain

- There are many phases of an attack
- Each phase represents a point of protection
- Each phase represents a point of failure
- Each phase represents a point of detection
- Each phase represents an opportunity to kill the attack in progress

Phase In The Cyber Kill Chain



Phases of an Attack

- Find
- Fix
- Track
- Target
- Engage
- Assess

The Human as a Choice Vector

- The attackers target humans as one potential vector of many
- Became a vector of choice
- Poor awareness
- Poor controls around the human
- Assume the organization has already been targeted, then the determine which people to target

Each Attack has Own Kill Chain

- Physical attacks use different methods and have different prevention, detection, and reaction strategies
- Policies, procedures, and guidelines must be identified for Protection, Detection, and Reaction
- Technology must be implemented as appropriate

10 Phases of The Phishing Kill Chain

- There are 10 opportunities to stop phishing attacks
- 9 within your control
- 7 technological
- 2 user related
- 10 phases to stop the attack

There are only two points at which a user is really at fault for a phishing attack.

Later Detection Can Feed Prevention

- Phishing typically launched against multiple targets simultaneously
- Messages can be clicked over weeks
- Early detection can remove unopened messages earlier in the kill chain than originally detected
- Can look for infections not prevented
- Mitigates successful attacks
- Important for future mitigation

Phishing Kill Chain

Pre-Mail Server

- Internet infrastructure should prevent phishing messages in the first place
- Perimeter devices can potentially filter some illicit messages

Mail Server

- Mail server should detect phishing messages
- Suspected messages should be quarantined
- Reports of phishing messages should result in unopened messages being deleted
- Payloads should be removed even if forwarded to users

Client Mail Application

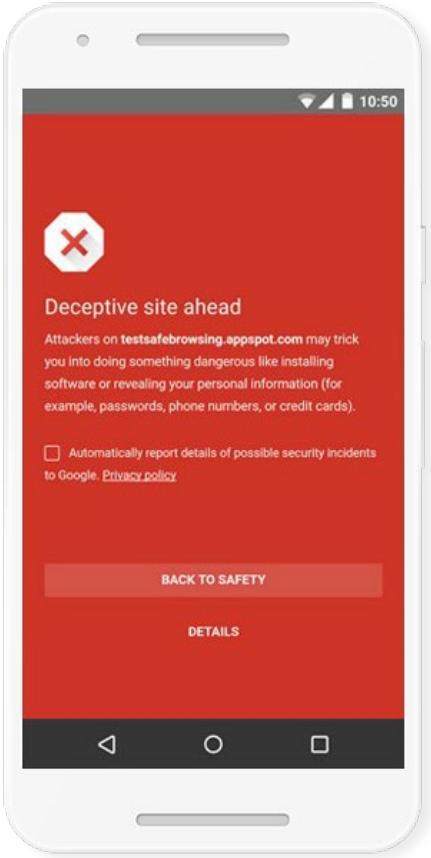
- Provides another layer of filters
- Quarantines suspected spam and phishing
- Frequently this is two layers
  - Mail application
  - Client anti-malware

User Review

- Message in the spam folder
  - The user can leave it there
  - The user can open it and take action
- Message in inbox
  - The user can perceive it as a phishing message
  - The user can take action

Mail Application Confirms Action

- The application should warn the user against action
- Ignore spam folder location
- Warn of clicking on link
- Warn of potential for malicious software
- Other warnings as appropriate

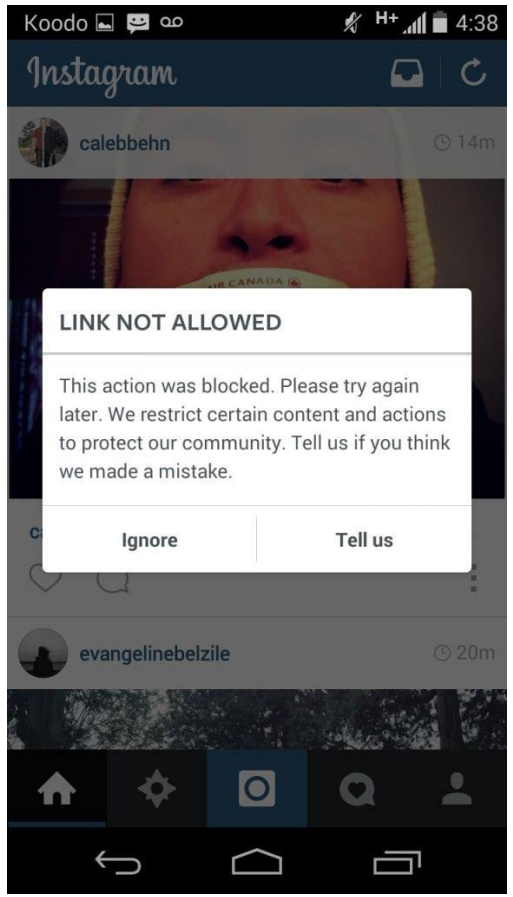


User Considers Warnings

- User considers if they really want to take the action
- Reports spam
- Deletes message

Client Prevents Attack

- Outside the mail application, the system prevents infections
- Stops malicious programs from loading
- Stops user from going to malicious links
- Warns if user attempts to send data to outside parties
- DLP
- Detects loading of keystroke loggers



Network Prevents Actions

- Beyond client, network should detect impact
- Sees uploading of files
- Web filters prevent malicious links
- Other preventative measures should stop a variety of actions

Network Detects Successful Attacks

- Intrusion detection and prevention should detect indications of attacks
- Data streams out of the network
- Illicit logon attempts should be detected
- There are always signs that should be found

Detected Compromises Should be Mitigated

- Once an attack is detected, it should be stopped
- Detection itself doesn't stop attacks

Kill Chain Summary

- Pre-mail server
- Mail server
- Client mail application
- User
- Client application warns user
- User confirms action
- Client prevents damage
- Network prevents damage
- Network detects attack
- Network mitigates attack

Backward Mitigation

- When an attack is detected, phishing allows for mitigation early in the kill chain
- Not all messages are opened at the same time
  - Might be opened over a week or more
  - Although most might be opened within an hour
- If user reports message to admins, admins can delete messages still unopened in user queues
- Domains can be blocked
- Malware can be detected and deleted

Successfully Stopping the Syrian Electronic Army

- They were mad at me for calling them cockroaches at RSAC 2014
  - The truth hurts
- They attacked RSA Conference, Wall Street Journal, and BuzzFeed
- Wrote article for Computerworld
- Threat intelligence defined how they would retaliate against Computerworld and parent company
- Warned users
- Users reported phishing messages
- Unopened messages deleted and domains blocked

Now That We're Here, Reverse Engineer

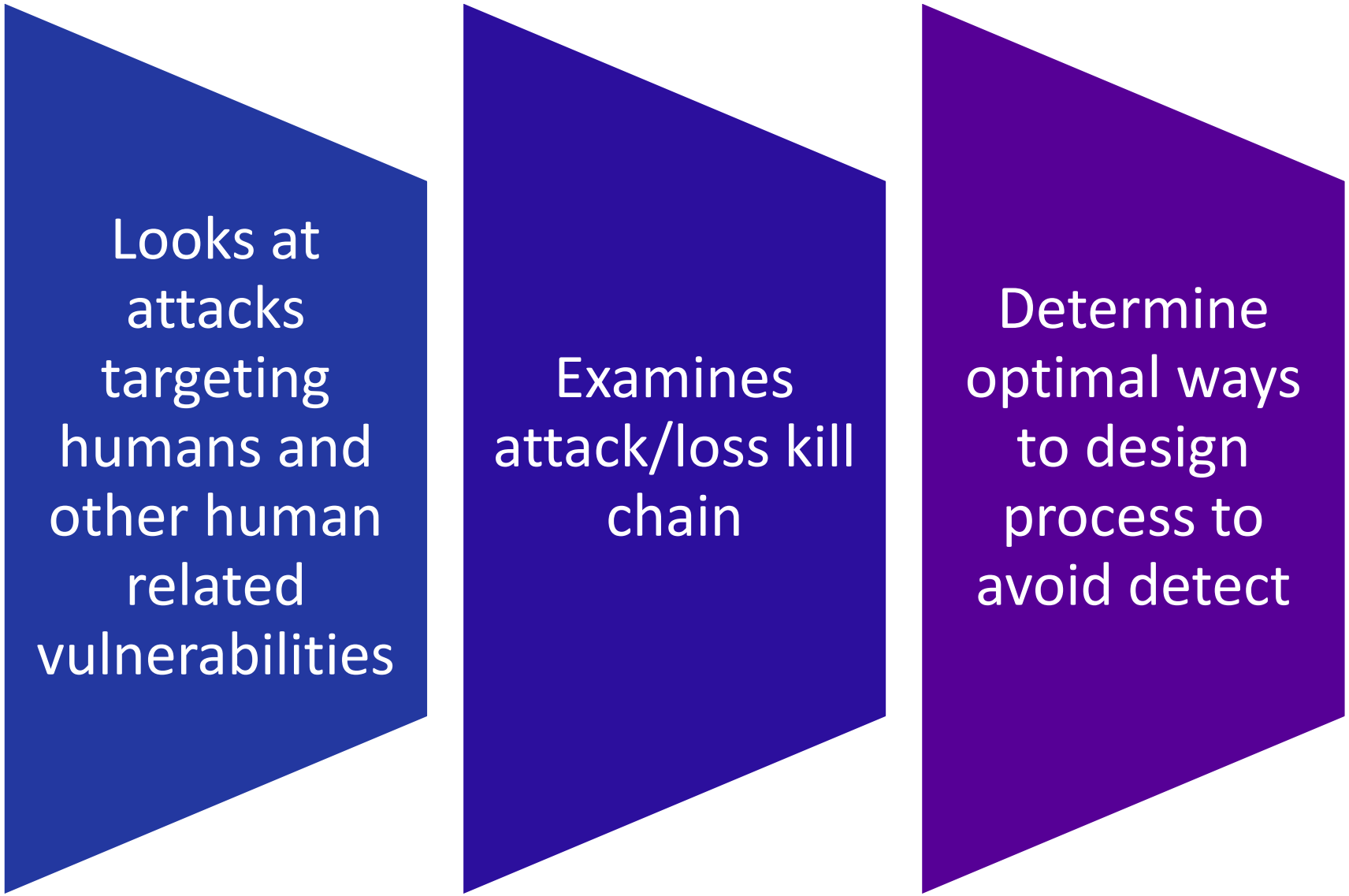
Dissecting the Attack

What vulnerabilities were exploited?	How was the attack detected?	How can we detect in the future?	How to counter the attack (immediate & downstream)

The Missing Piece…Process

- Governance is generally a stack of documents
- Need to determine where decisions are made
  - Reduce decisions
  - Define decisions
- Look to technology to reduce exposure or mitigate user actions
- Process implemented through technology
- Process defined to users

The Human Security Officer



HSO Actions

Coordinated Response	• …after kill chain examination
Technology	• Prevent attacks from getting to humans • Mitigating attacks after bad user actions
Procedures/Guidelines for user decision	• Remove decisions • Define decisions to remove discretion
Awareness	• Promote defined behaviors • Some general awareness

Which One Are You Creating?

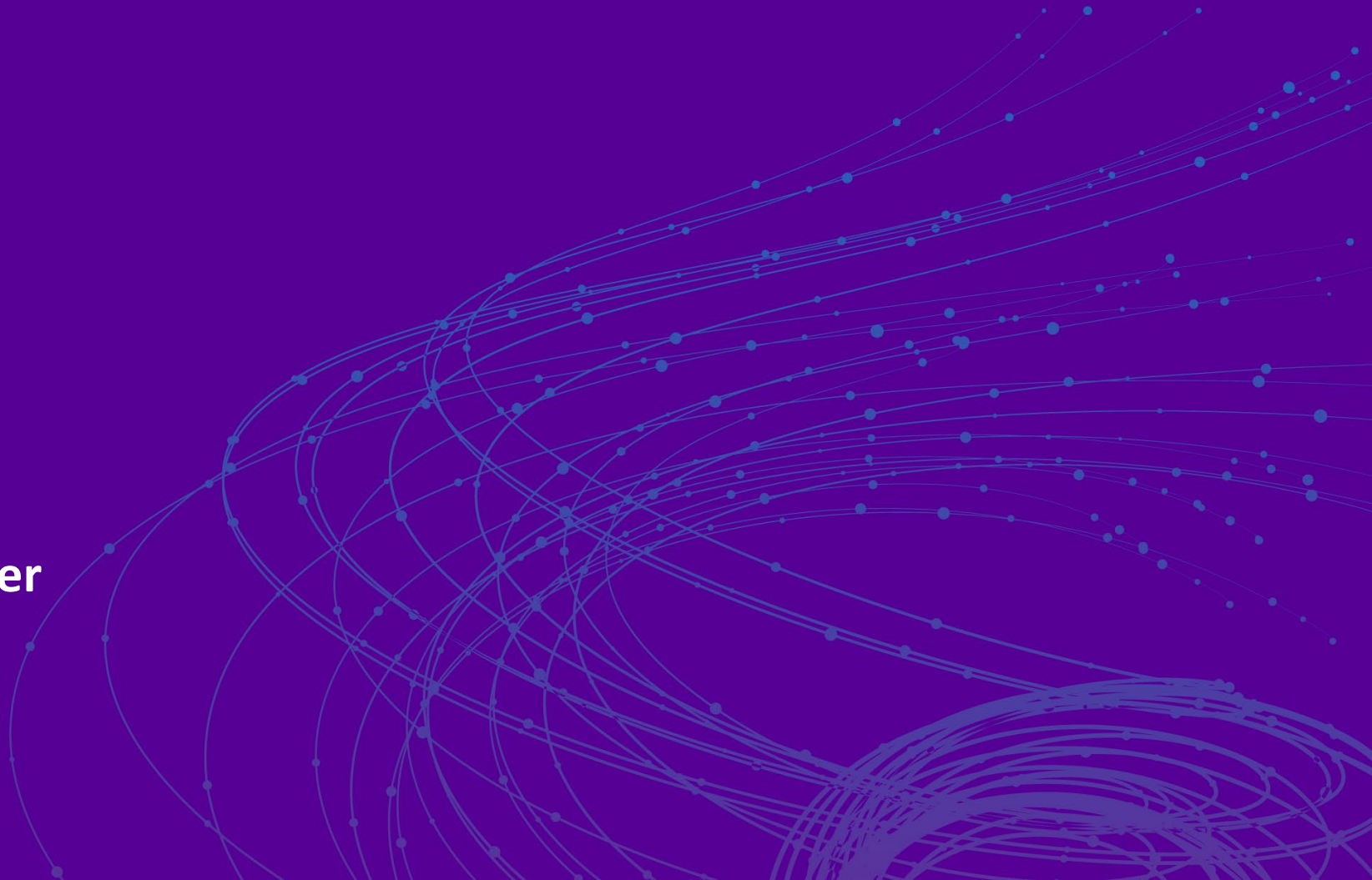
Summary

- Acknowledge user failure is not just a user failure
- There needs to be specific coordination of mitigating attacks and losses involving people
- There are Chief Network Architects, Chief Data Architects, etc. Why not HSOs?
- It is much more than awareness

RSAConference2019

APPLY

Let’s Bring It In Closer



Creating A Kill Chain

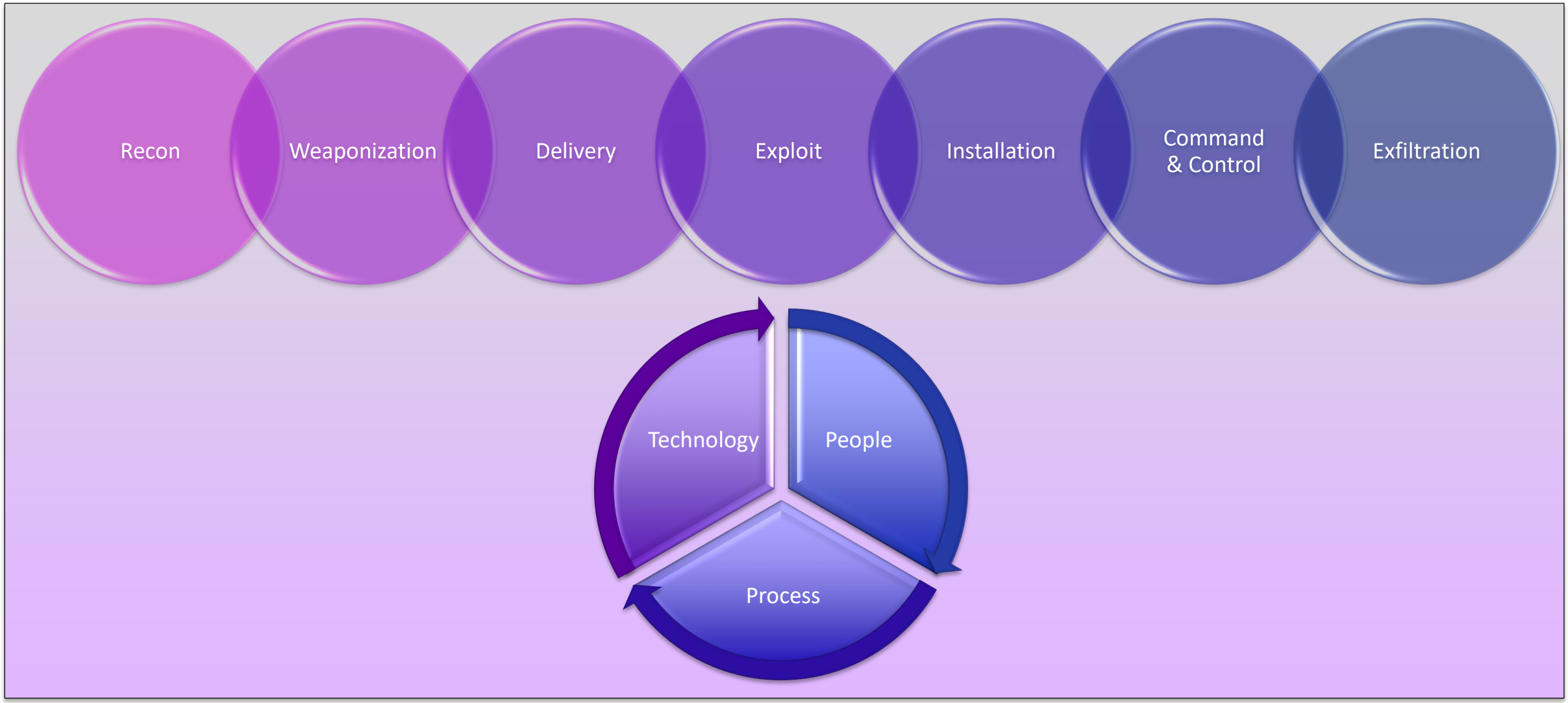
- Find the human to attack
- How is the human targeted?
- Identify the type of attack to execute
- How does the user enable the attack?
- How can the attack be stopped?

Assignment

- Define possible attacks
- Assign different attacks to different tables
- Define the potential kill chain
- Define the potential countermeasures
- Come up with a holistic approach
- Report to group
- Determine potential commonalities
  - As a group

ATTACKS?

Phases In The Cyber Kill Chain



Kill Chain Summary

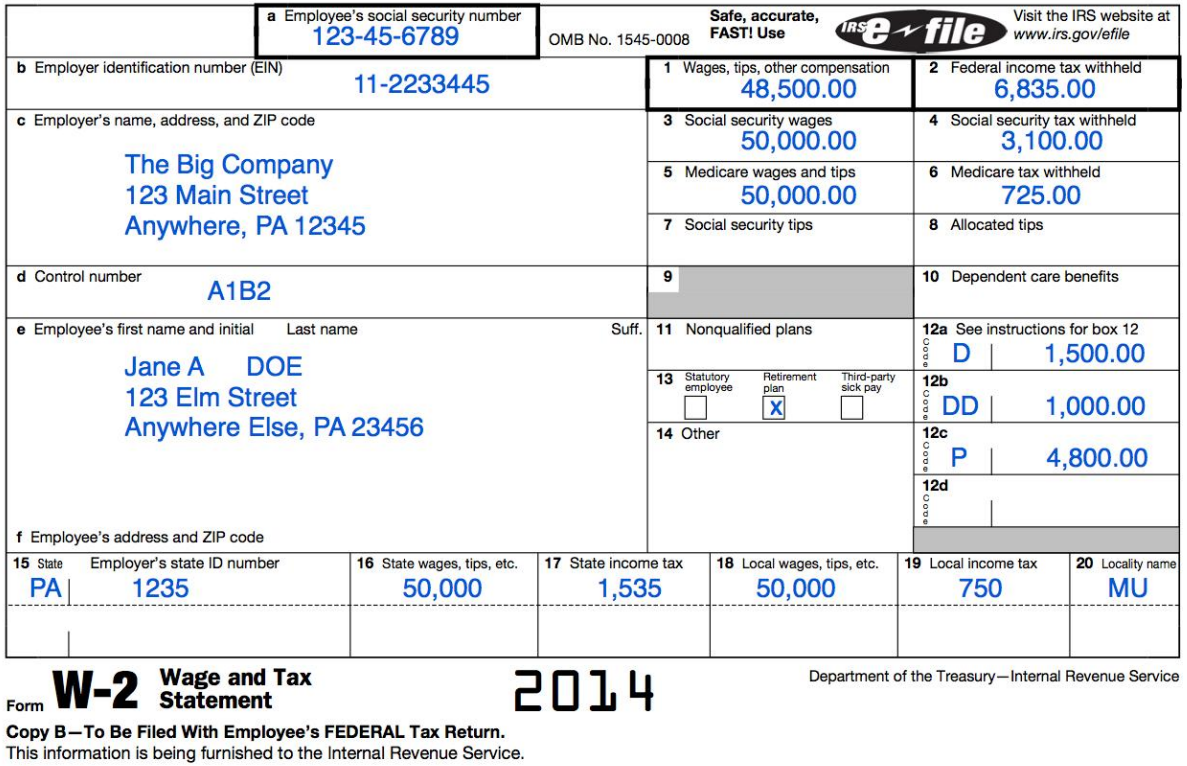
- Pre-mail server
- Mail server
- Client mail application
- User
- Client application warns user
- User confirms action
- Client prevents damage
- Network prevents damage
- Network detects attack
- Network mitigates attack

REPORTS

COMMONALITIES

Examples

- W-2 Fraud
- Malware
- Tailgating



a Employee's social security number: 123-45-6789
OMB No. 1545-0008
Safe, accurate, FAST! Use — IRS e-file — Visit the IRS website at www.irs.gov/efile

b Employer identification number (EIN): 11-2233445
1 Wages, tips, other compensation: 48,500.00
2 Federal income tax withheld: 6,835.00

c Employer's name, address, and ZIP code:
The Big Company
123 Main Street
Anywhere, PA 12345

3 Social security wages: 50,000.00
4 Social security tax withheld: 3,100.00
5 Medicare wages and tips: 50,000.00
6 Medicare tax withheld: 725.00
7 Social security tips
8 Allocated tips

d Control number: A1B2
9
10 Dependent care benefits

e Employee's first name and initial: Jane A — Last name: DOE — Suff.
123 Elm Street
Anywhere Else, PA 23456

11 Nonqualified plans
12a See instructions for box 12 — Code D | 1,500.00
13 Statutory employee ☐ Retirement plan ☒ Third-party sick pay ☐
12b Code DD | 1,000.00
14 Other
12c Code P | 4,800.00
12d Code

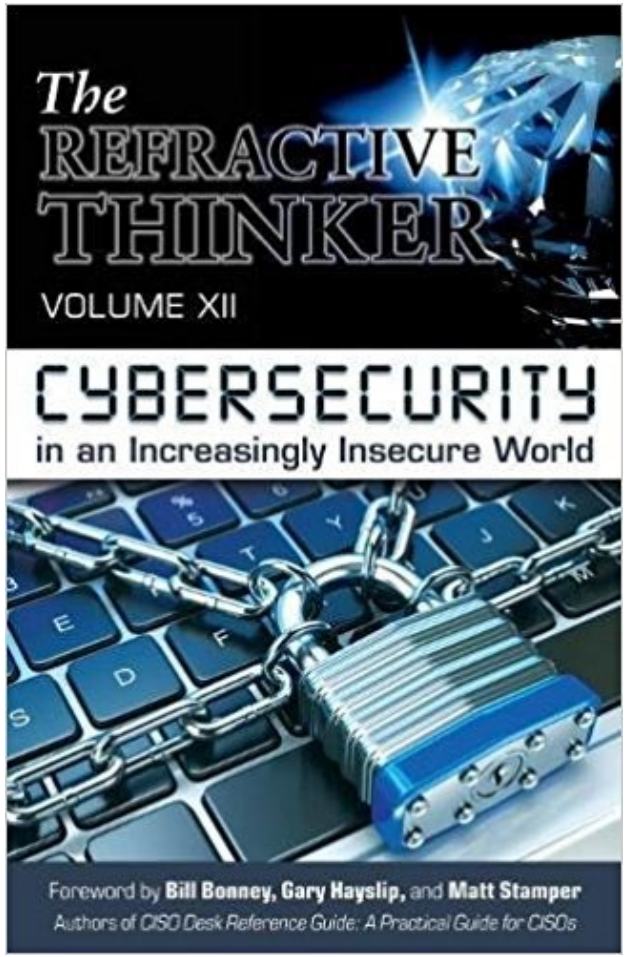
f Employee's address and ZIP code

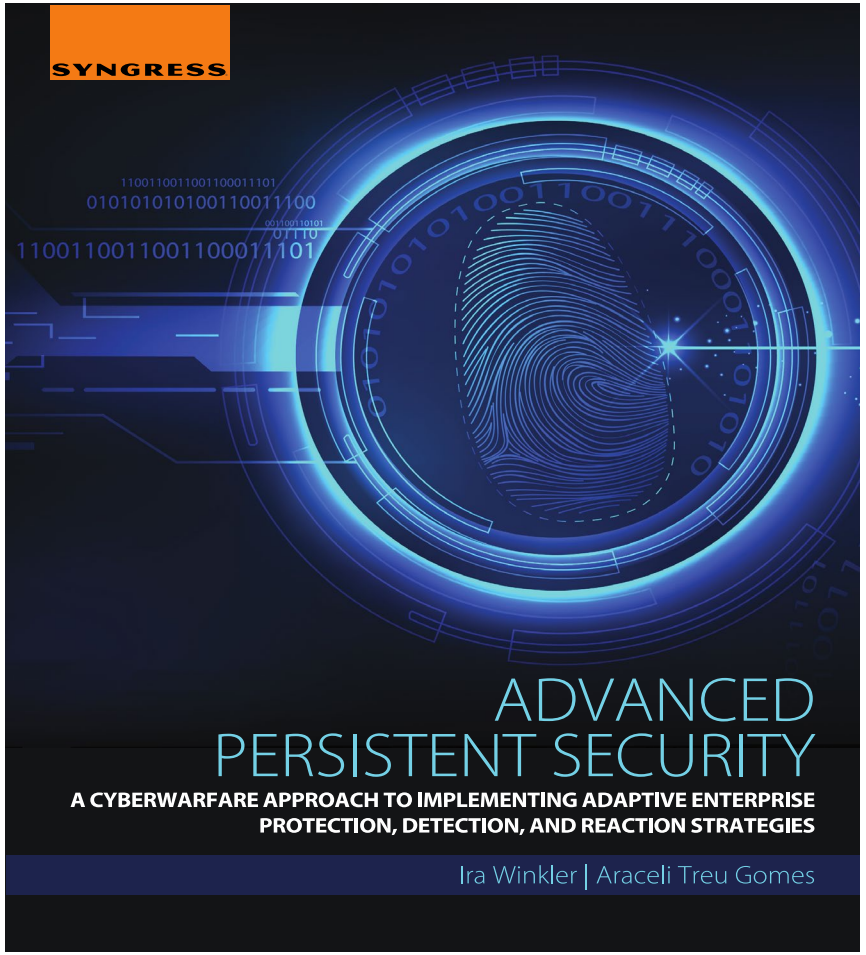
15 State	Employer's state ID number	16 State wages, tips, etc.	17 State income tax	18 Local wages, tips, etc.	19 Local income tax	20 Locality name
PA	1235	50,000	1,535	50,000	750	MU

Form W-2 Wage and Tax Statement 2014
Department of the Treasury—Internal Revenue Service

Copy B—To Be Filed With Employee's FEDERAL Tax Return.
This information is being furnished to the Internal Revenue Service.

The Books, The Myths, The Legends





This Is Us

Ira Winkler, CISSP

- ira@securementem.com
- @irawinkler
- www.securementem.com
- www.linkedin.com/in/irawinkler

Tracy Celaya, DM, CISSP

- tracy@startwithgo.com
- @DrTracyC
- www.tracycelaya.com
- www.linkedin.com/in/tracycelaya

Alexandra Panaretos

- Alexandra.Panaretos1@ey.com
- @Cyber_Simple
- https://www.linkedin.com/in/alexandra-panaretos

RSAConference2019

Questions?

Password Attack

- Password is identified: brute force, social engineering, post-it note…
- System access is gained; network, data, executables, etc.
- Detect by identifying malicious behavior
- Counters:
  - Lockout
  - Complexity
  - Frequency
  - Social media policy to mitigate engineering
  - Password policy (clean desk, no clues, etc)

Other Types of Attacks

- Spear-Phishing
- Drive-By
- Surfing
- Denial-of-Service
- Eavesdropping
- Malware
- Tailgating
- Man-in-the-Middle