RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **RMG-02**

Creating and Implementing a Behavioral Cybersecurity Program

Ira Winkler

Chief Security Architect
Walmart
@irawinkler

What is Behavioral Cybersecurity?

- Poorly defined
- Roughly the implementation of behavioral science, psychology, and cognitive science to enhance cybersecurity programs
- At first glance, it is about security awareness
- It can, and should, be much more

What Should Behavioral Cybersecurity Be?

- End user behavioral risk reduction
  - Awareness and otherwise
- Customer sentiment, as appropriate
- Improving cybersecurity professional practices
- Improving wellness of the professional staff
- Research of relevant principles

Why a Discipline?

- Too much Bro-science out there
- It is more than reading Cialdini or BJ Fogg, or taking an NLP class
- Behavioral science is an established discipline
- Involves research and training
- User experience is as, maybe more, important as psychological gimmicks
- Tremendous benefit to be realized beyond awareness

RSAConference2022

End-User Behavior Improvement

Security Awareness

- Statistical analysis of campaign effectiveness
- Determining how to implement scientific principles into awareness programs
- Improving phishing assessments through metrics and behavioral principles
- Looking to additional methods of awareness delivery

Implementing Gamification

- More than a game
- Reward system to reward behaviors in practice
- Understand how to reward people
- Determine what to reward
- Tracking points
- Modifying program based on results

User Experience

- Leading people to make better decisions regardless of awareness
- Nudges to make better decisions
- Modifying interfaces to improve behaviors
- Statistical analysis to determine where user failings happen
- Determining data accesses and permissions to provide and reduce
- Process improvement

See You Can Stop Stupid or Human Security Engineering presentations

Procedure Improvement

- Analyze end user functions to embed cybersecurity practices
- Optimize practices to simplify and reduce errors
- Definition of practices within procedures and guidelines
- Promote the proper practices

Awareness should be how to do work properly, not what to be afraid of

Human Incident Response

- Why did the incident happen?
- Why did the user initiate loss?
- What were the awareness failings?
- What were the systematic failings?
- Plan and implement countermeasures

RSAConference2022

Customer Sentiment

Who Are Your Customers?

- Beyond your users
- B2C
- B2B

User Experience

- Is your security user friendly?
- Is your password policy a nightmare?
- Does the experience provide a perception of security?

Providing Enhanced Security

- Going beyond the purpose
- Provide resources to enhance overall security
- Tools
- Knowledge

Public Relations

- Promote what you're doing

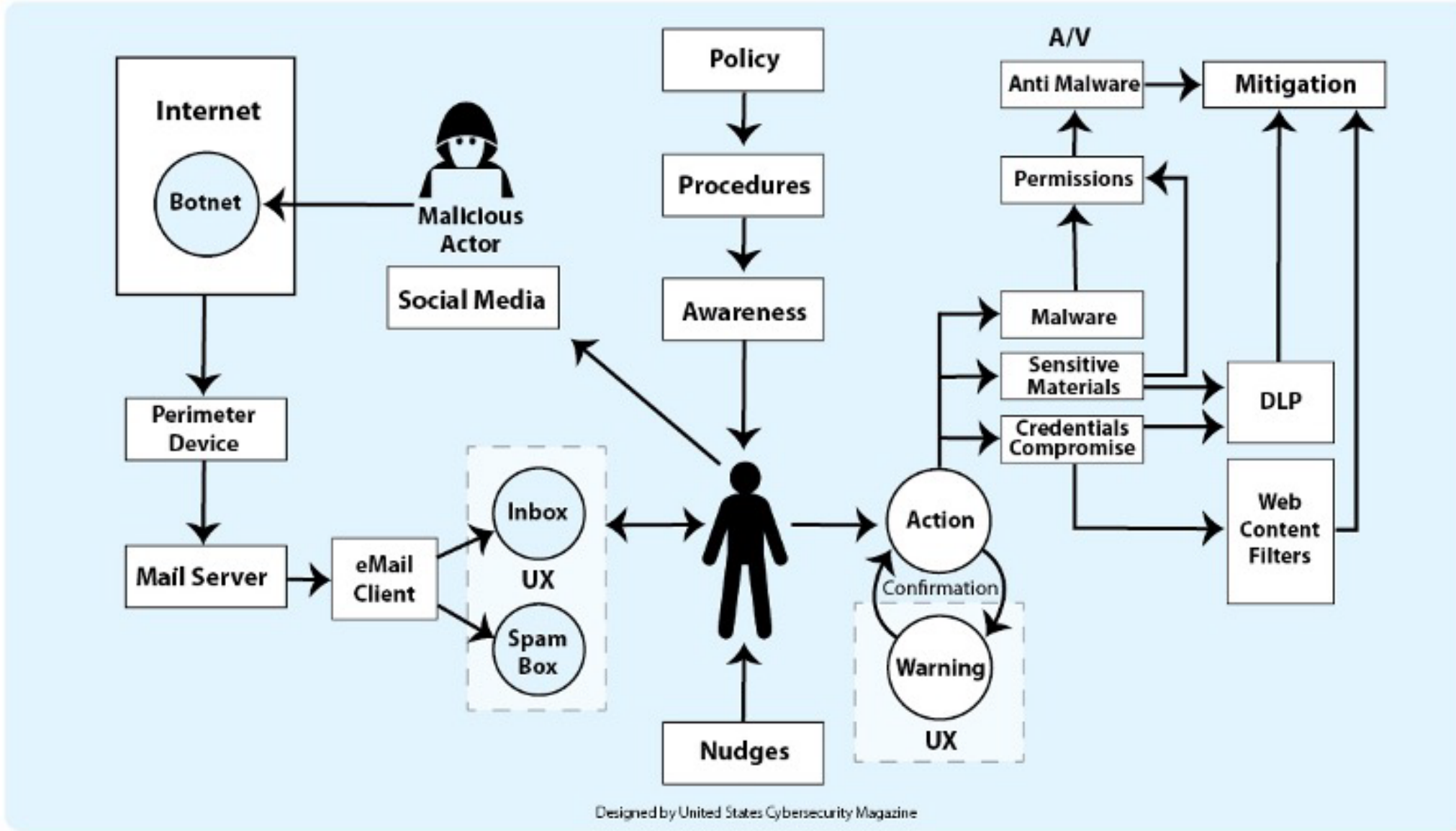
RSAConference2022

Improving Cybersecurity Practices

Where Can You Enhance Practices?

- Where are bad cybersecurity decisions made?
- Where can decisions making be improved?
- Where can practices be improved?

HUMAN SECURITY ENGINEERING MODEL PHISHING PREVENTION



User Experience

- Cybersecurity tool usability
- How is information displayed?
- Reducing information presented to cybersecurity professionals
- Analysis of error rates
- Optimizing information displays

Training and Certification

- What training is required to improve performance?
- Certifications?
- Tracking and mapping of skills
- Guiding for career progression
- Guiding for team needs
- Soft skills?
- Looking forward

Recruiting

- Determining needs
- Positioning organization and cybersecurity team
- Identifying candidates
- Rating candidates
- Streamlining hiring process

RSAConference2022

Improving Professional Wellness

A Widely Known Problem

- Burnout
- Stress
- Anxiety

Addressing the Issues

- Implementing employee wellness targeted to cybersecurity personnel
- Meditation training
- Scheduling of events to alleviate stress
- Regular wellness checks

RSAConference2022

Research

Depends Where it is Needed

- Determine shortfalls
- Look into funding university and other research programs that have potential
- Science exists that needs to be brought into practice
- Culture
- Enhanced awareness
- Behavior modification
- Error reduction

RSAConference2022

Logistics

Staff Composition

- Data scientists
  - First by intent
- Programmers
- Project managers
- Behavioral scientists
- Doctoral researchers
- Awareness practitioners
- Trainers

Training

- The disciplines identified
- Communications skills
- Research methodologies
- Data science
- Statistical analysis

Partnerships

- Human Resources
- Physical Security
- Employee Wellness
- Awareness
- Training
- Operations
- Data Science
- Others as logical

RSAConference2022

Putting it All Together

Create an Umbrella

- Some efforts likely being implemented
- Many efforts should be part of the general CISO function
  - Almost a Chief of Staff function
- Consolidate tracking of what exists under the program
- See what's working and what isn't
- Be mindful of internal politics

Determine Available Resources

- Who do you have available?
- What level of funding do you have?
- Do you have the relationships in place to execute what you need?
- What resources beyond funding are available?
- What is your skillset?

Choosing the Projects

- Where is the best use of your resources?
- Where is the most visible impact to be made?
- Where will you have the least resistance?
- Can you make the most use of the effort?
- Finite or ongoing?

Always Collect Metrics

- Measure all efforts in all categories
  - See my books for metrics
- Behavioral science is treated like Bro-science too often
- Implement scientific rigor to prove value, OR stop wasting money
- Prove your value, as incidents will happen
- Justify your existence

“Apply” Slide

- Next week you should:
  - Identify relevant efforts that qualify as Behavioral Cybersecurity
- In the first three months following this presentation you should:
  - Determine if you can create an umbrella for your efforts
  - Identify potential efforts beyond awareness to pursue
  - Seek support and funding
- Within six months you should:
  - Create a common dashboard for efforts under your umbrella
  - Compile Day 0 metrics to show your future impact
  - Begin an additional effort; even minor, like Human Incident Response procedures

Thank You!!!

www.facebook.com/ira.winkler

@irawinkler

www.linkedin.com/in/irawinkler

We’re Hiring; A Lot

www.Walmart.com/careers