MEDIAPRO®
Learn. Improve. Succeed.

The Challenge of Creating an Adaptive Awareness Program

Tom Pendergast, Ph.D.
Chief Strategist
MediaPro

Outline

The Tier 4 Challenge

The Adaptive Awareness Framework

Putting the Framework into Action

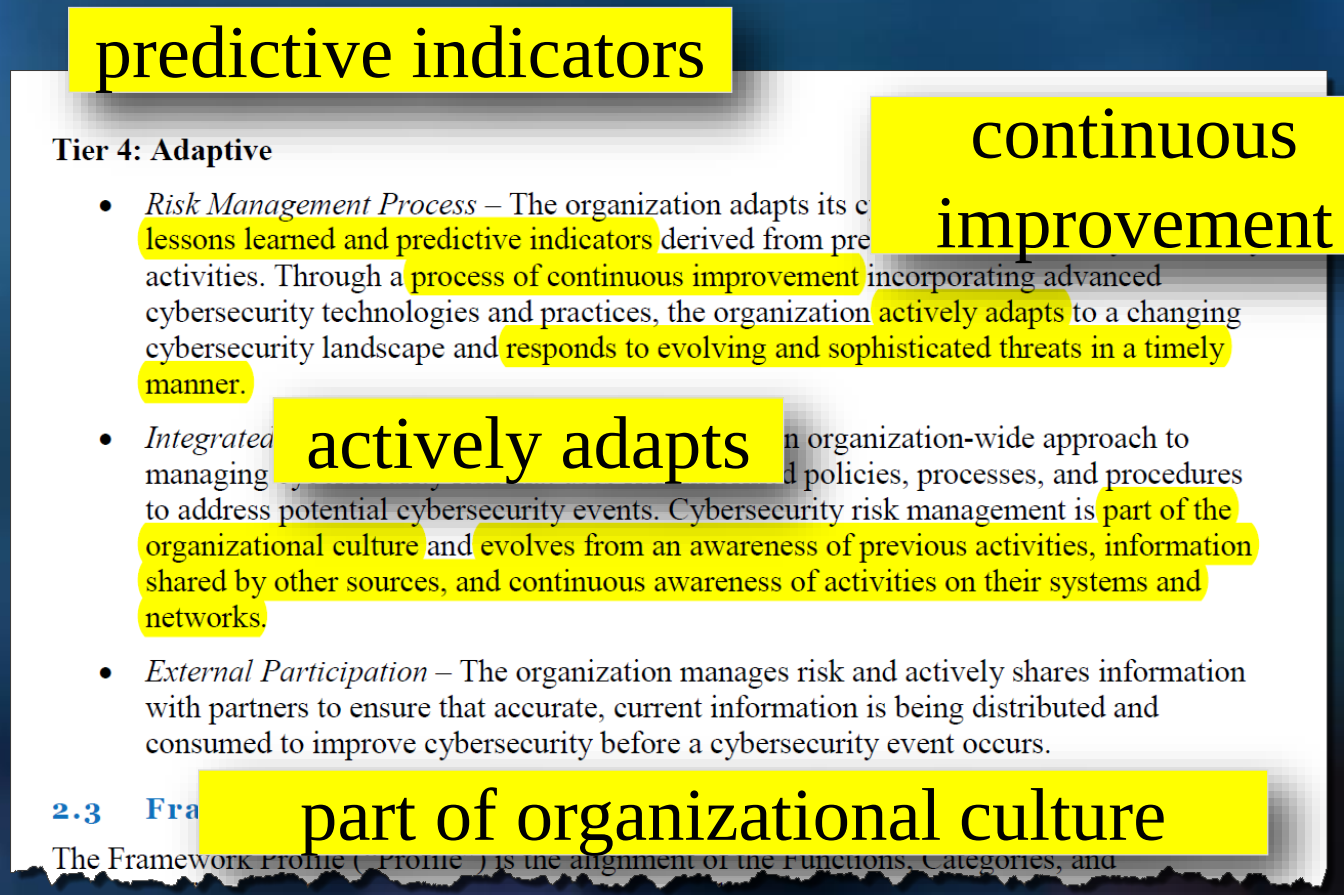
The Tier 4 Challenge

Predictive Indicators

Continuous Improvement

Adapts and Responds

Part of the Culture



Adaptive Awareness

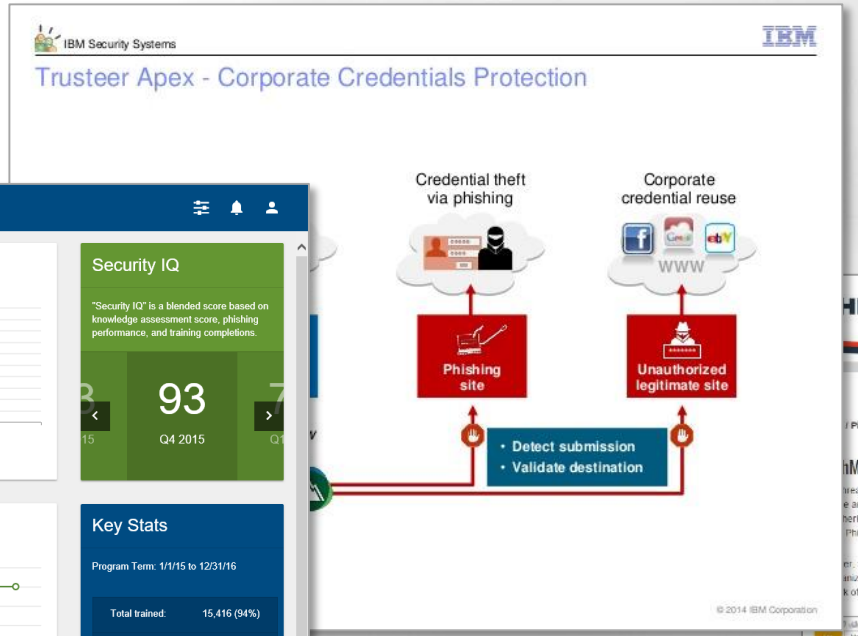
Analyze

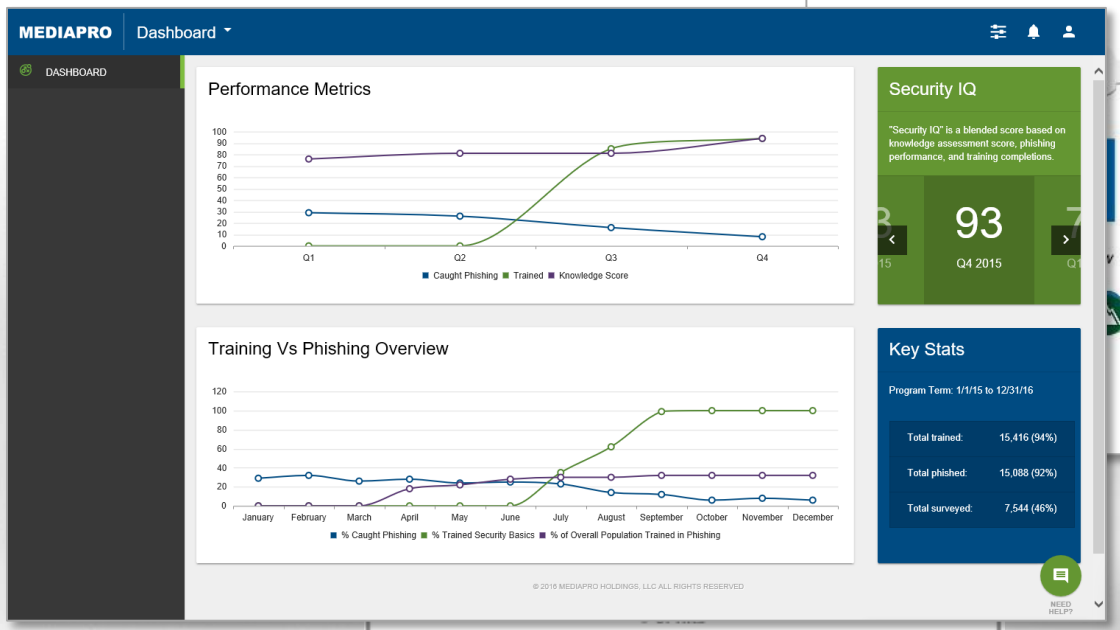
Plan

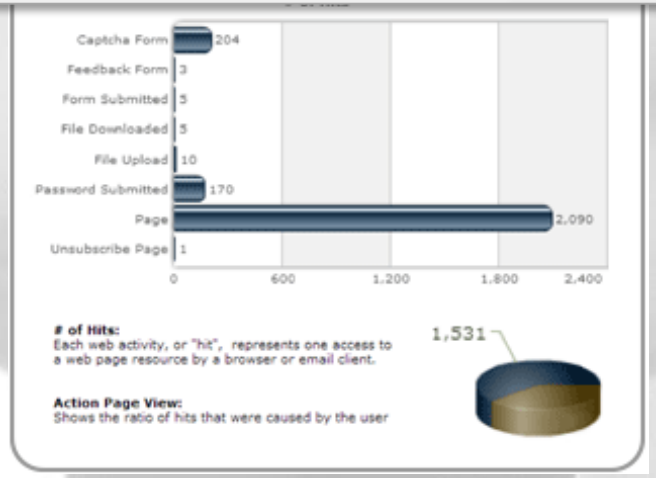
Train

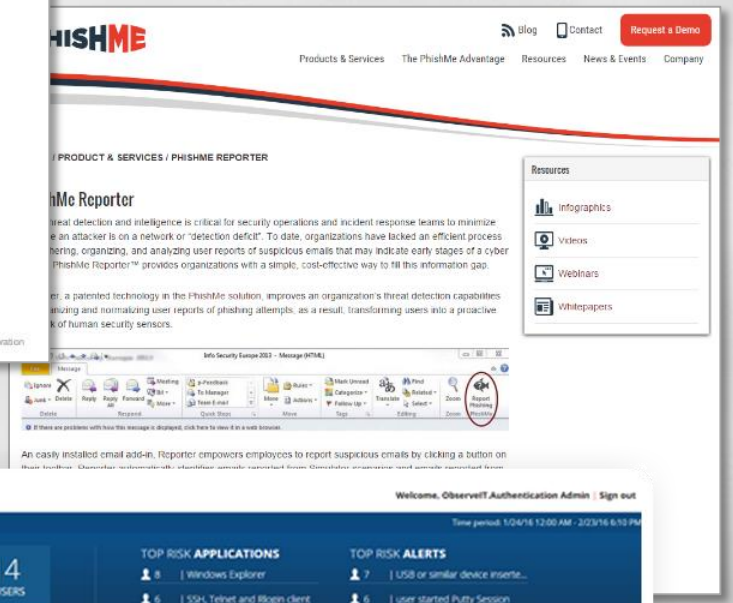
Reinforce

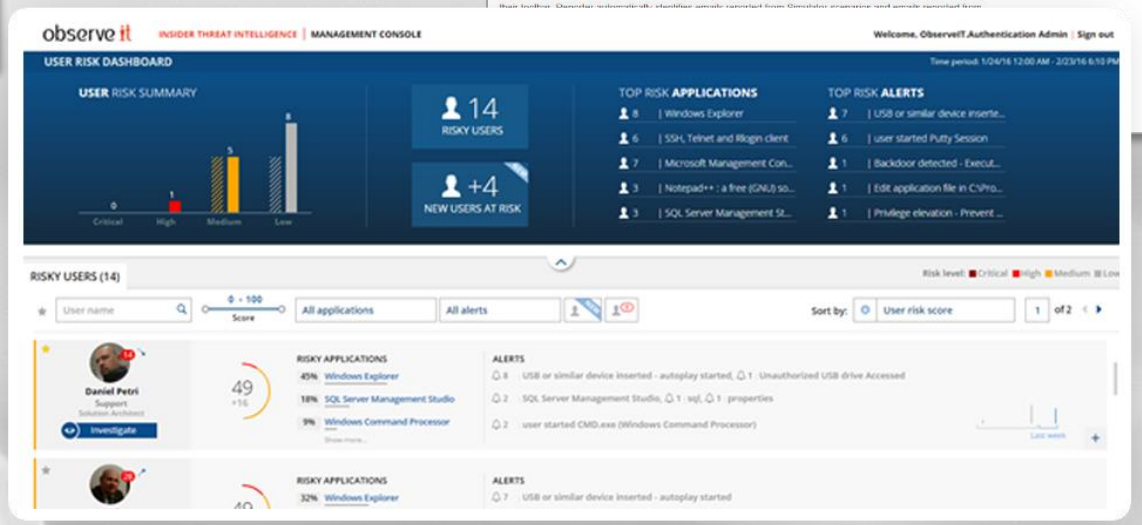
Analyze


IBM Security Systems
IBM
Trusteer Apex - Corporate Credentials Protection
Credential theft via phishing
Corporate credential reuse
Phishing site
Unauthorized legitimate site
www
• Detect submission
• Validate destination
© 2014 IBM Corporation


MEDIAPRO
Dashboard
DASHBOARD
Performance Metrics
Caught Phishing
Trained
Knowledge Score
Security IQ
"Security IQ" is a blended score based on knowledge assessment score, phishing performance, and training completions.
93
Q4 2015
Training Vs Phishing Overview
% Caught Phishing
% Trained Security Basics
% of Overall Population Trained in Phishing
Key Stats
Program Term: 1/1/15 to 12/31/16
Total trained: 15,416 (94%)
Total phished: 15,088 (92%)
Total surveyed: 7,544 (46%)
© 2016 MEDIAPRO HOLDINGS, LLC ALL RIGHTS RESERVED

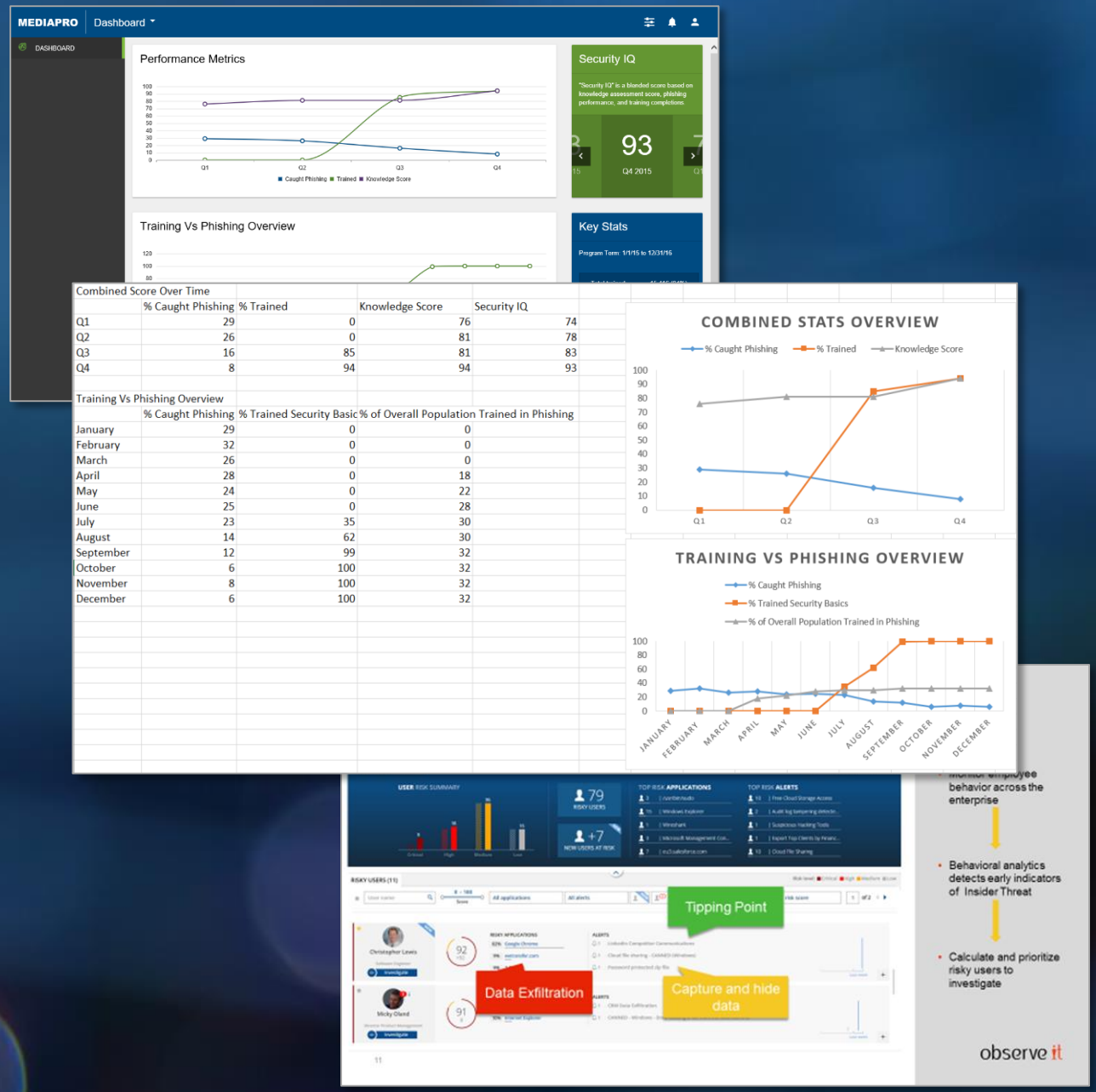

Captcha Form 204
Feedback Form 3
Form Submitted 5
File Downloaded 5
File Upload 10
Password Submitted 170
Page 2,090
Unsubscribe Page 1
# of Hits:
Each web activity, or "hit", represents one access to a web page resource by a browser or email client.
Action Page View:
Shows the ratio of hits that were caused by the user
1,531


PHISHME
Blog
Contact
Request a Demo
Products & Services
The PhishMe Advantage
Resources
News & Events
Company
Resources
Infographics
Videos
Webinars
Whitepapers

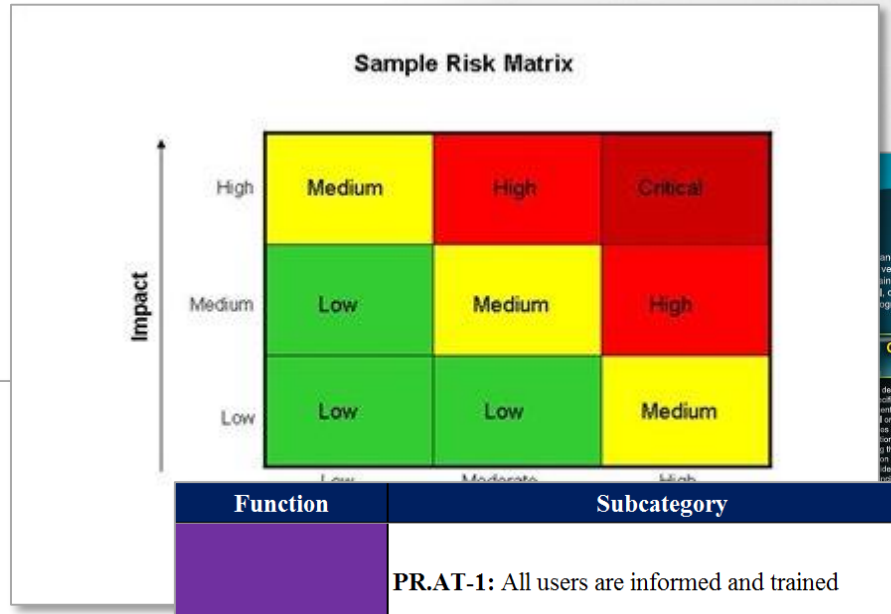

observe it
INSIDER THREAT INTELLIGENCE | MANAGEMENT CONSOLE
USER RISK DASHBOARD
USER RISK SUMMARY
14
RISKY USERS
+4
NEW USERS AT RISK
TOP RISK APPLICATIONS
TOP RISK ALERTS
RISKY USERS (14)

Analyze Options

- Surveys
- Phishing / Social Engineering
- Behavioral Analytics
- Incident Reporting
- Completion Rates
- Other?

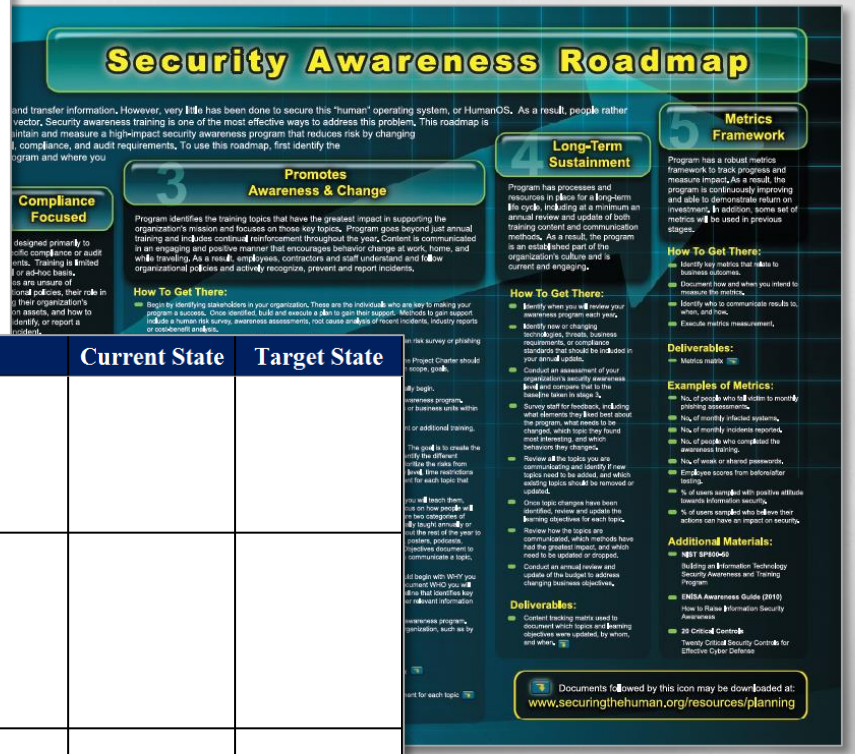


Plan

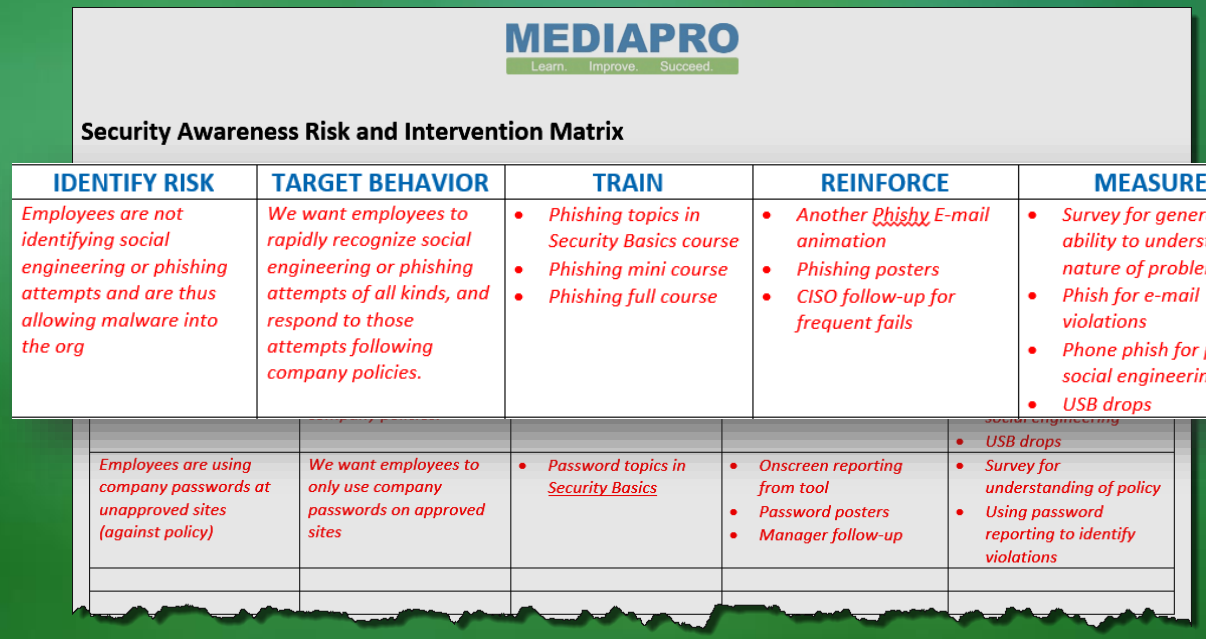


MEDIAPRO
Learn. Improve. Succeed.

Security Awareness Planning Toolkit



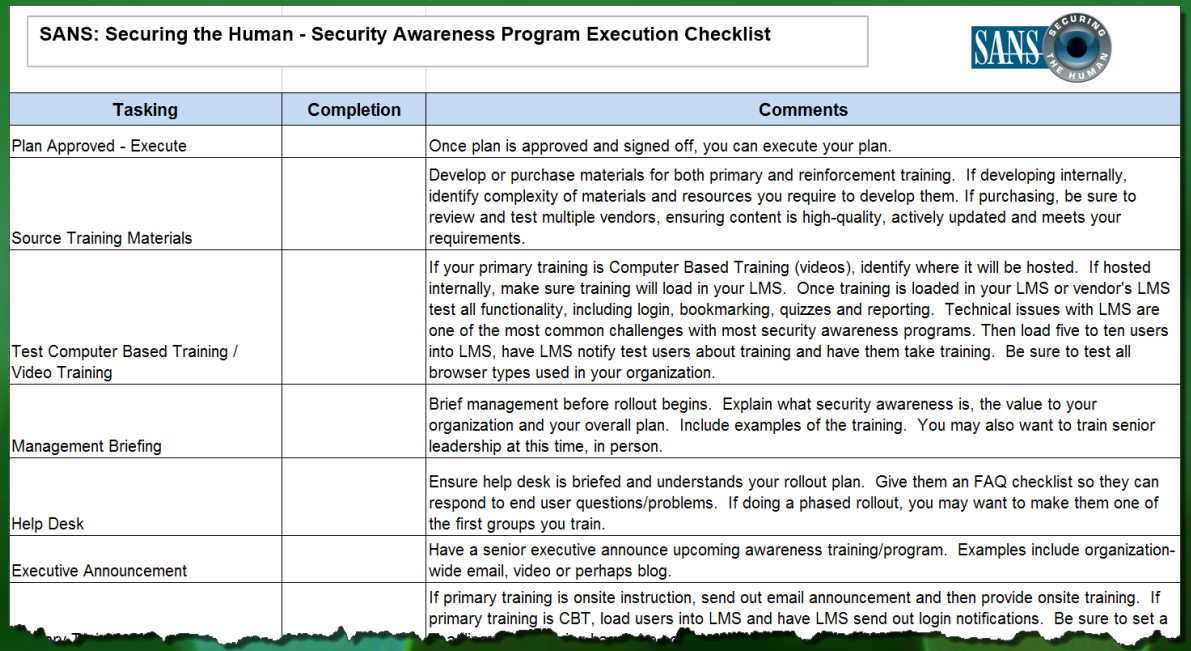
Function	Subcategory	Current State	Target State
	PR.AT-1: All users are informed and trained		
	PR.AT-2: Privileged users understand roles & responsibilities		
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities		



MEDIAPRO
Learn. Improve. Succeed.

Security Awareness Risk and Intervention Matrix

IDENTIFY RISK	TARGET BEHAVIOR	TRAIN	REINFORCE	MEASURE
Employees are not identifying social engineering or phishing attempts and are thus allowing malware into the org	*We want employees to rapidly recognize social engineering or phishing attempts of all kinds, and respond to those attempts following company policies.*	• *Phishing topics in Security Basics course* • *Phishing mini course* • *Phishing full course*	• *Another Phishy E-mail animation* • *Phishing posters* • *CISO follow-up for frequent fails*	• *Survey for general ability to understand nature of problem* • *Phish for e-mail violations* • *Phone phish for phone social engineering* • *USB drops*
				• *USB drops*
Employees are using company passwords at unapproved sites (against policy)	*We want employees to only use company passwords on approved sites*	• *Password topics in Security Basics*	• *Onscreen reporting from tool* • *Password posters* • *Manager follow-up*	• *Survey for understanding of policy* • *Using password reporting to identify violations*



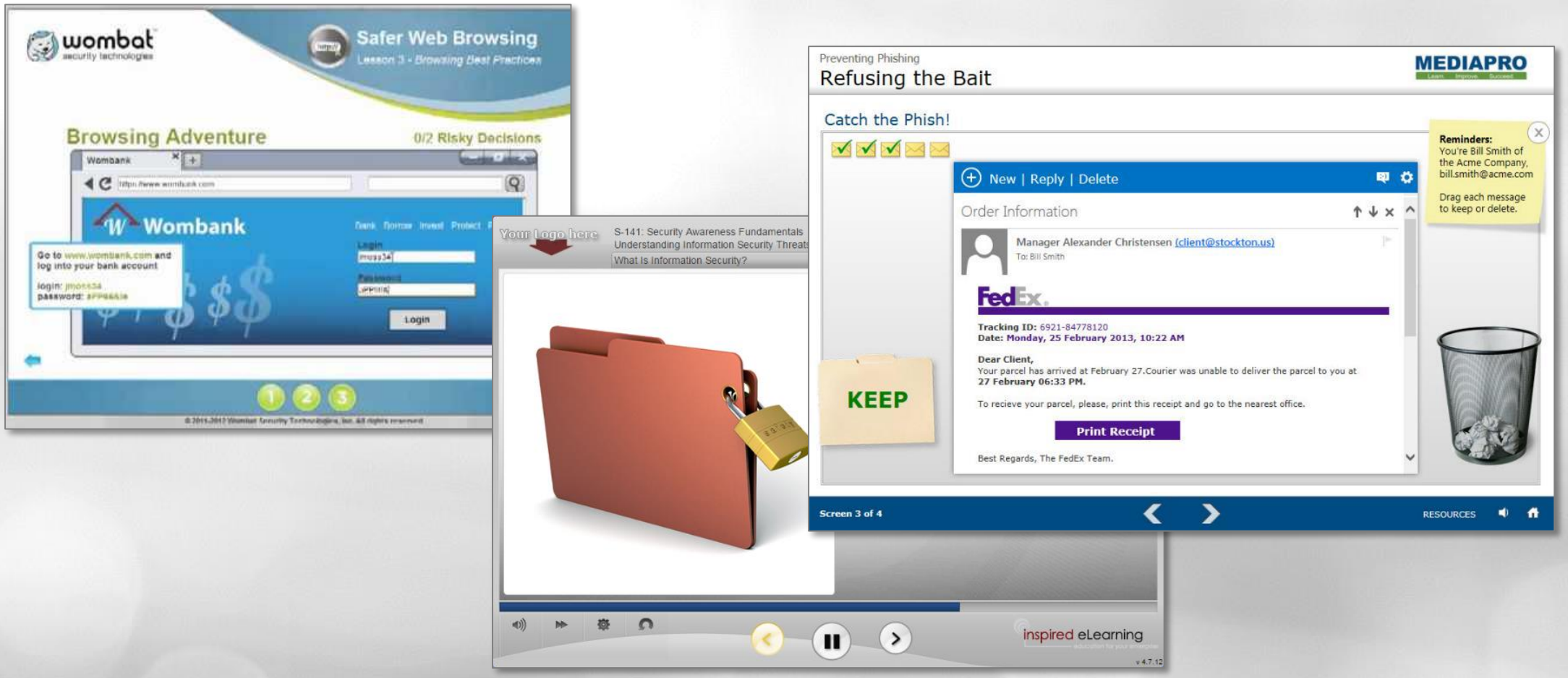
SANS: Securing the Human - Security Awareness Program Execution Checklist

Tasking	Completion	Comments
Plan Approved - Execute		Once plan is approved and signed off, you can execute your plan.
Source Training Materials		Develop or purchase materials for both primary and reinforcement training. If developing internally, identify complexity of materials and resources you require to develop them. If purchasing, be sure to review and test multiple vendors, ensuring content is high-quality, actively updated and meets your requirements.
Test Computer Based Training / Video Training		If your primary training is Computer Based Training (videos), identify where it will be hosted. If hosted internally, make sure training will load in your LMS. Once training is loaded in your LMS or vendor's LMS test all functionality, including login, bookmarking, quizzes and reporting. Technical issues with LMS are one of the most common challenges with most security awareness programs. Then load five to ten users into LMS, have LMS notify test users about training and have them take training. Be sure to test all browser types used in your organization.
Management Briefing		Brief management before rollout begins. Explain what security awareness is, the value to your organization and your overall plan. Include examples of the training. You may also want to train senior leadership at this time, in person.
Help Desk		Ensure help desk is briefed and understands your rollout plan. Give them an FAQ checklist so they can respond to end user questions/problems. If doing a phased rollout, you may want to make them one of the first groups you train.
Executive Announcement		Have a senior executive announce upcoming awareness training/program. Examples include organization-wide email, video or perhaps blog.
		If primary training is onsite instruction, send out email announcement and then provide onsite training. If primary training is CBT, load users into LMS and have LMS send out login notifications. Be sure to set a

Planning Options

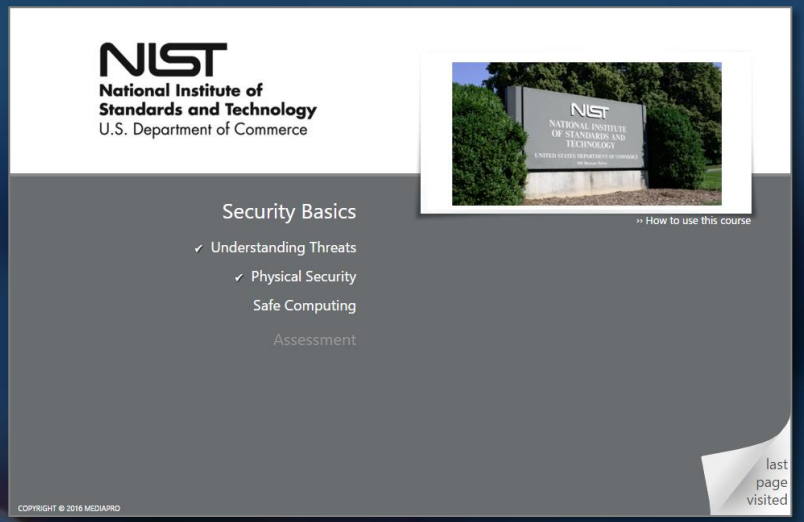
- Identify Risks
- Target Behaviors
- Identify Tools (Training and Reinforcement)
- Plan to Measure
- Plan to Change

Train


wombat
security technologies
Safer Web Browsing
Lesson 3 - Browsing Best Practices
Browsing Adventure
0/2 Risky Decisions
Wombank
Wombank
Go to www.wombank.com and log into your bank account
Login
Your Logo here
S-141: Security Awareness Fundamentals
Understanding Information Security Threats
What is Information Security?
inspired eLearning
Preventing Phishing
Refusing the Bait
MEDIAPRO
Catch the Phish!
New | Reply | Delete
Order Information
Manager Alexander Christensen (client@stockton.us)
To: Bill Smith
FedEx.
Tracking ID: 6921-84778120
Date: Monday, 25 February 2013, 10:22 AM
Dear Client,
Your parcel has arrived at February 27.Courier was unable to deliver the parcel to you at 27 February 06:33 PM.
To recieve your parcel, please, print this receipt and go to the nearest office.
Print Receipt
Best Regards, The FedEx Team.
KEEP
Reminders:
You're Bill Smith of the Acme Company, bill.smith@acme.com
Drag each message to keep or delete.
Screen 3 of 4
RESOURCES

Training Options

- Online or In-Person
- Build vs Buy
- Easy to Refresh/Customize
- Required or Not?
- Behavioral?



Reinforce


Spike
Good dog
Bad password
Use Strong Passwords
MEDIAPRO

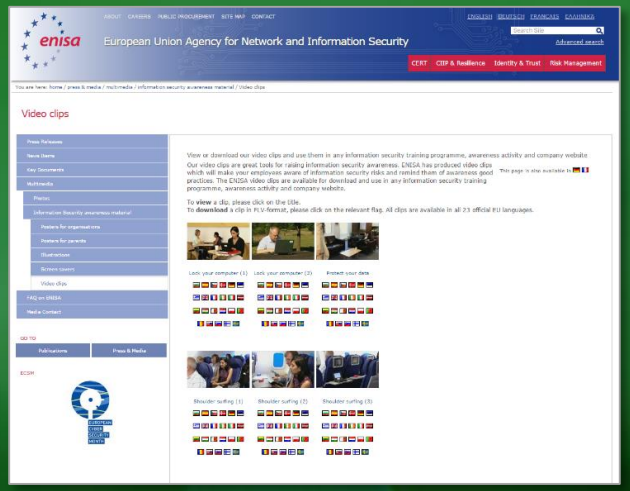

SANS
YOU ARE A TARGET
Username & Passwords
You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!, a security newsletter designed to help people just like you.
www.securingthehuman.org/ouch
Identity Hijacking
Web Server
Email Harvesting
Financial
Virtual Goods
Extortion
Botnet

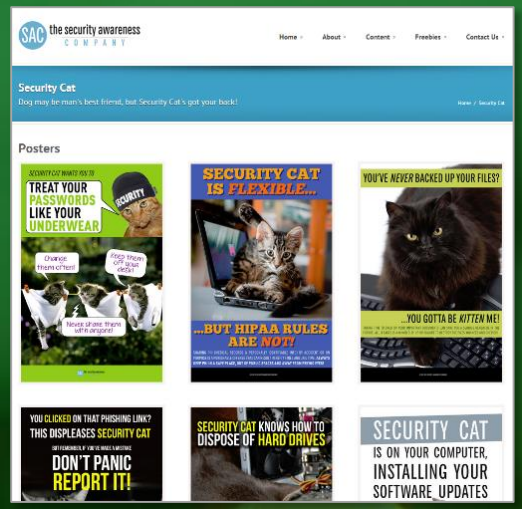

SECURITY HEADQUARTERS
As soon as I break through these firewalls, I will have all their privacy data!
The Security Trap Game
1
Question number


RSA CONFERENCE


SANS
OUCH! | May, 2015
OUCH!
IN THIS ISSUE
Securing the Cyber Generation Gap
Guest Editor
Overview
The Basics


ONE PERSON'S TRASH IS AN IDENTITY THIEF'S TREASURE
MEDIAPRO





Reinforcement Options

- Cost
- Cultural Fit
- Logistics

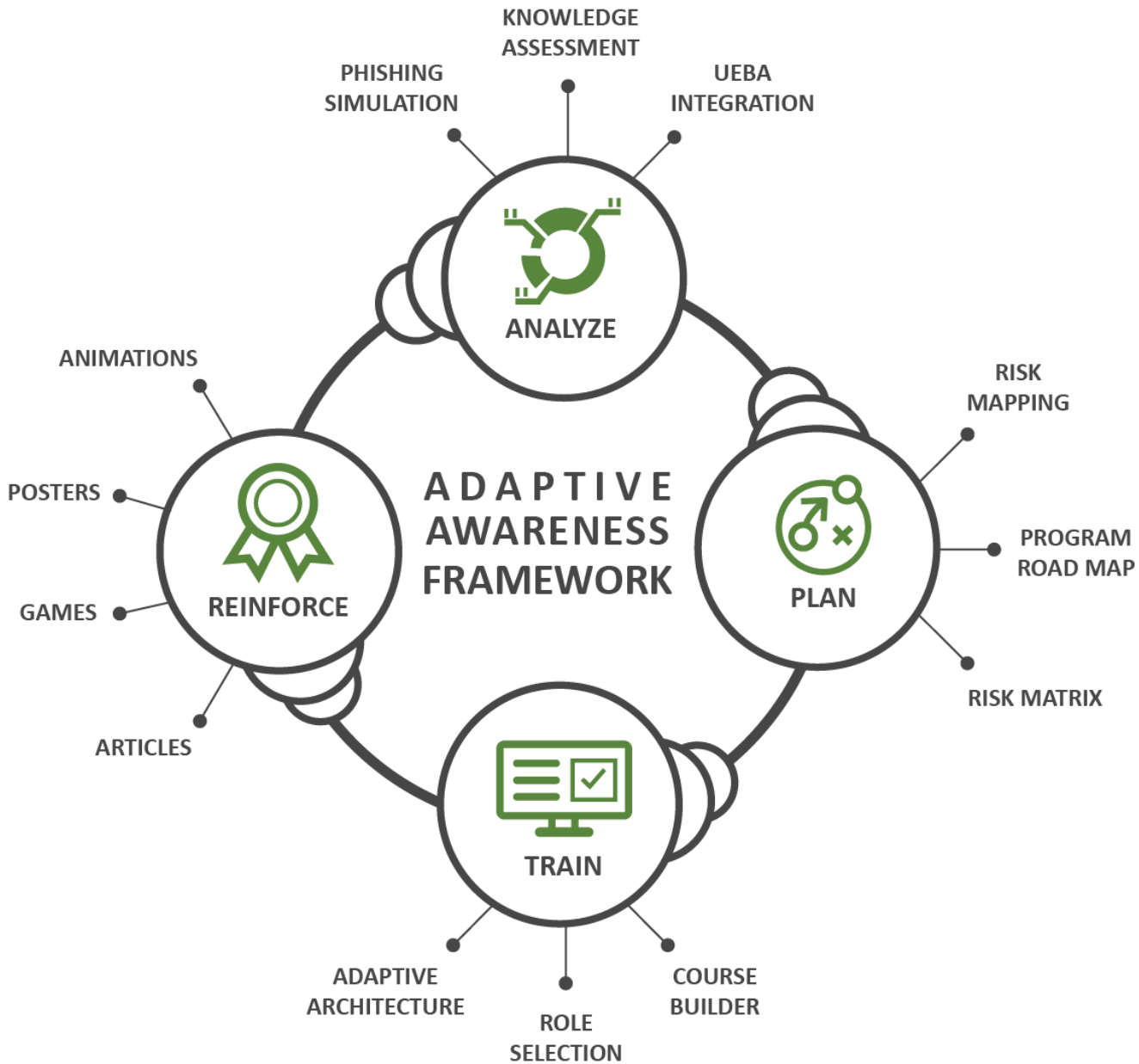
Putting It All Together

Start with data: survey, phish, etc.
Draft a plan with flexibility in mind
Announce the program (and keep it positive)
Train
Reinforce continuously
Analyze and Adapt

- Keep gathering data
- Reinforce when identifying problems (phishing, UBA)
- Make it relevant (role-based)
- Use personal follow-up messages to reinforce pressure points

Thank You!

Tom Pendergast
tomp@mediapro.com
425-483-4734


KNOWLEDGE ASSESSMENT
PHISHING SIMULATION
UEBA INTEGRATION
ANALYZE
ANIMATIONS
POSTERS
GAMES
ARTICLES
REINFORCE
ADAPTIVE AWARENESS FRAMEWORK
RISK MAPPING
PROGRAM ROAD MAP
RISK MATRIX
PLAN
TRAIN
ADAPTIVE ARCHITECTURE
ROLE SELECTION
COURSE BUILDER