fissea
FEDERAL
CYBERSECURITY | INNOVATION . AWARENESS . TRAINING

June 27 -29, 2019

BACH: Adaptive Cybersecurity Awareness Training using Artificial Intelligence

Dr. PAUL WANG
Endowed Chair

Dr. SHANE GALLAGHER
Researcher

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Cyber Awareness Training

Current efforts

- Text-based Training
  - Multiple choices, T/F
- Video Training
  - Watch pre-recorded videos
- Phishing Training
  - Generate phishing emails and wait people to click/download.

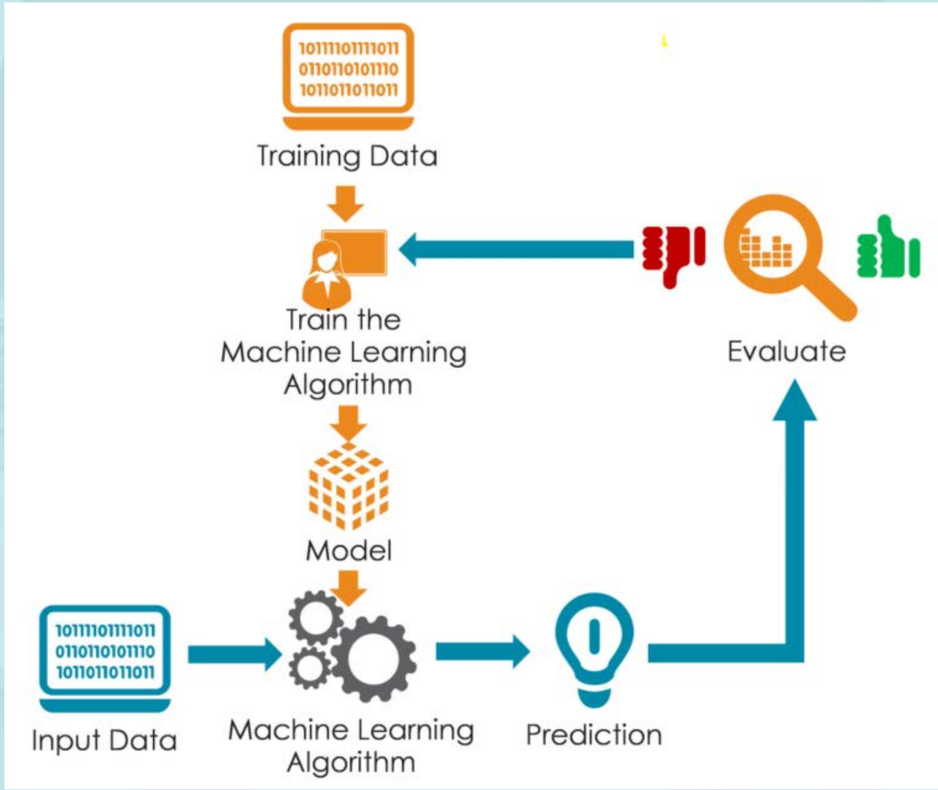
The Challenge

Improvement needed?

- ❖ Effective only in the beginning stage
  - No adaptation with the training
- ❖ Video may be too long
  - Less interesting and hard to follow
- ❖ Limited phishing tactics
  - Less effective with time

BACH – A Branch -AI-Charge Hybrid method in Cyber Awareness Training

- Combines adaptive learning methodology
- Interdisciplinary research technique
- Gamification of learning
- Artificial Intelligence (AI)

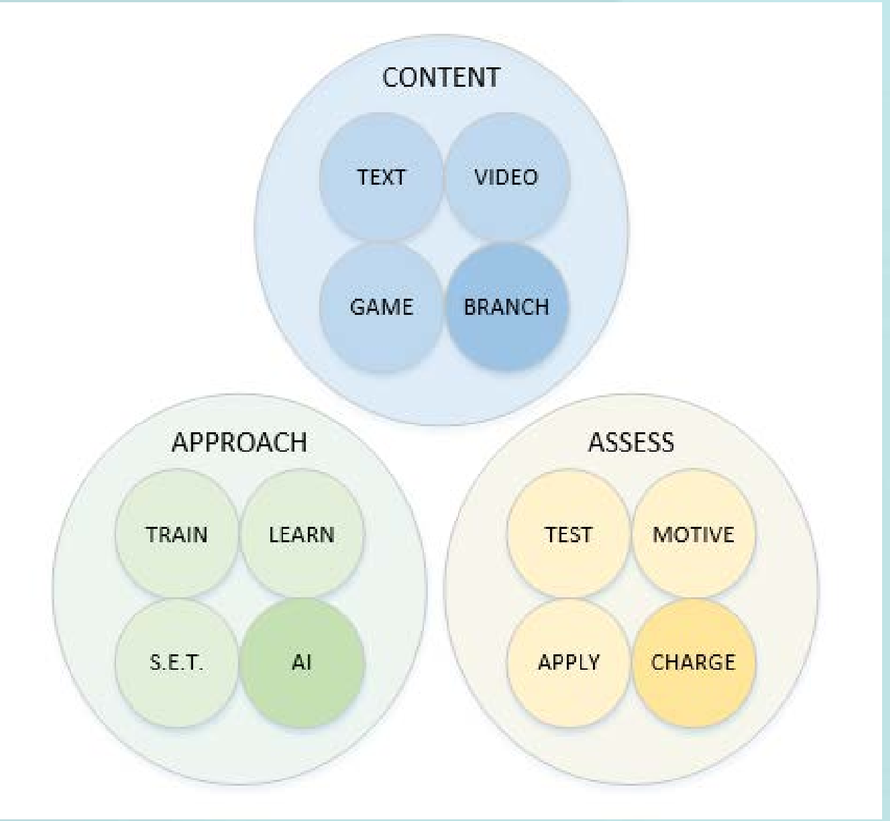


Amazon Web Services (AWS) AI Services

Approach

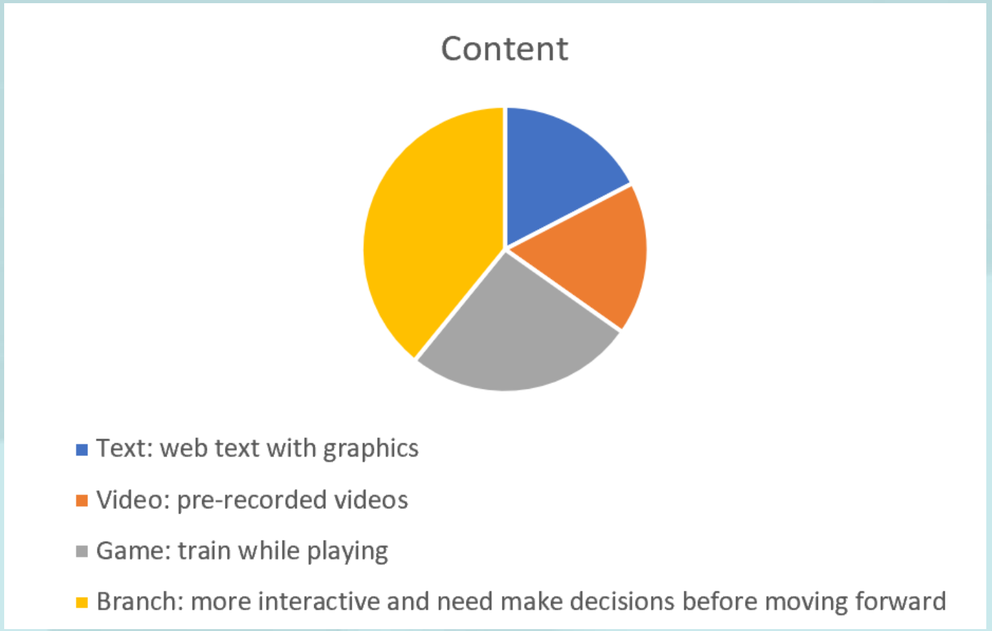
Four groups

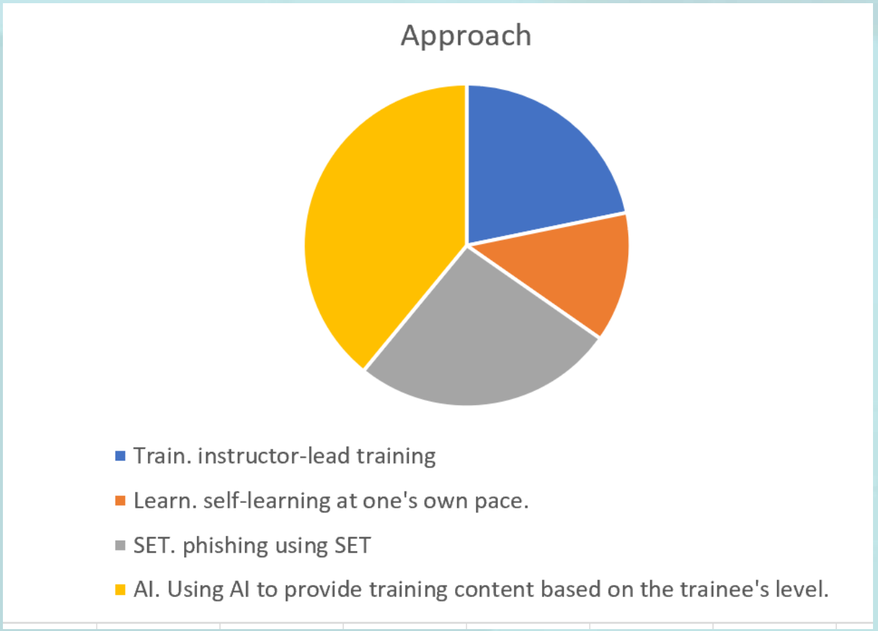
- Training in three categories: Content, Approach, and Assessment
- Each category is divided into four areas
  - Content: text, video, game, branch (non-linear)
  - Approach: train, learn, SET (social engineering), AI
  - Assessment: test, motive, apply, charge (in-charge training)
- Each group test one area

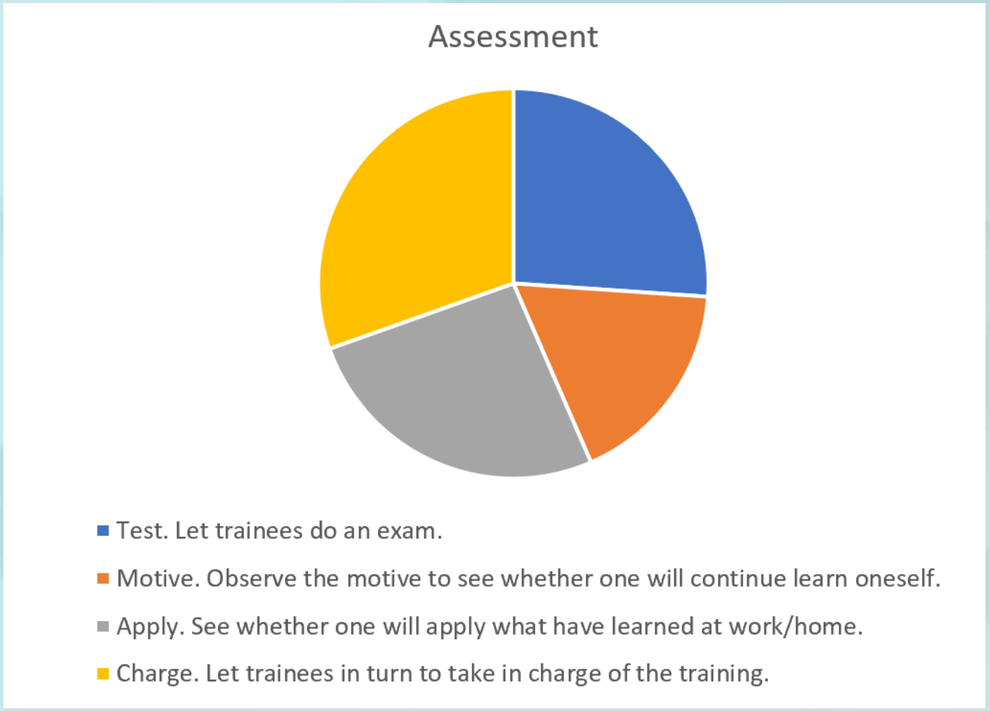


Experiments & Results

Total 24 students







Conclusions

- **Content**-wise, **Branched** material yield best training results.
  - Branch: more interactive and need make decisions before moving forward
- As for training **approach**, **AI** augmented **adaptive** training is most effective
  - AI: using AI to provide training content based on the trainee's level.
- For **assessment** method, let trainees to be in **charge** of the training is better
  - Charge: Let trainees in turn to be in charge of the training)

QUESTIONS? COMMENTS?

LET US KNOW!

EMAILs

paul.wang@computer.org, shane@sg-systems.com