WOLF & COMPANY, P.C.

# Overcoming Layer 8 Control Failures: Engaging your staff in the fight against cyber criminals

# Bio

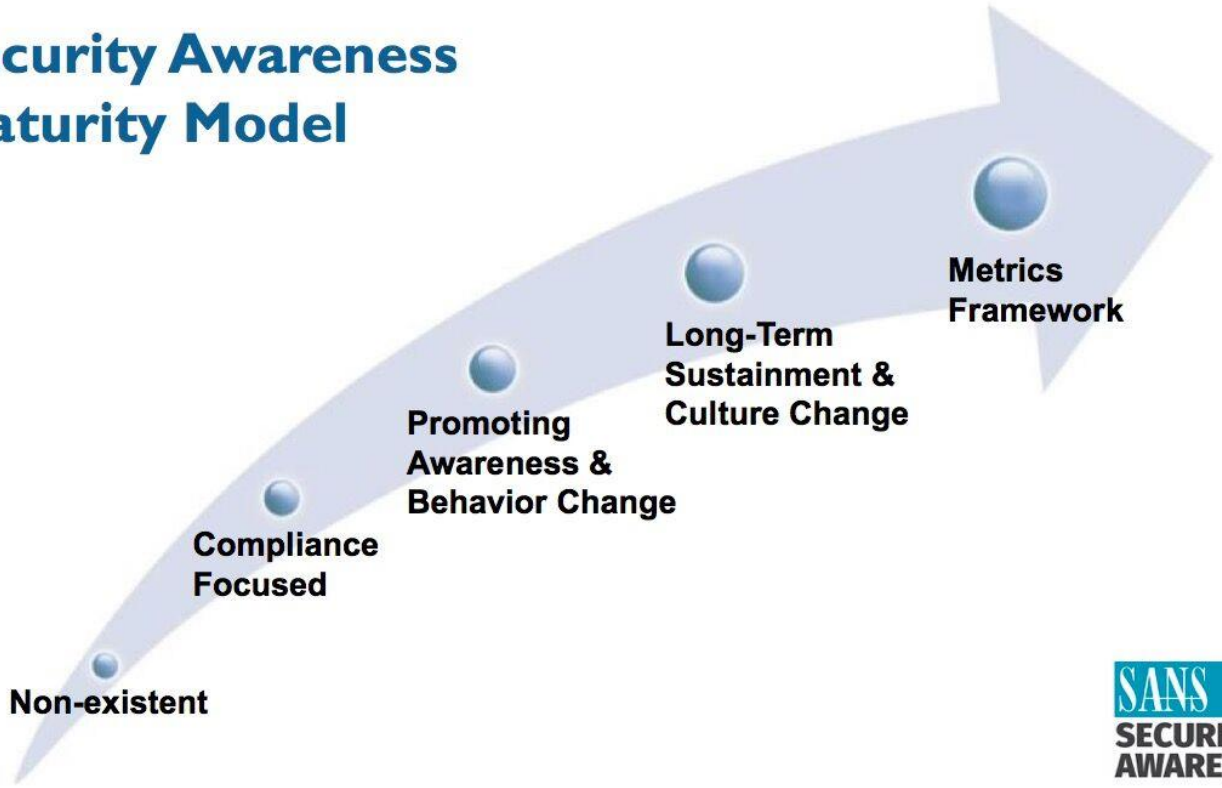
- Sean D. Goodwin
- CCSP | CISA | CISSP | GCCC | GCIA | GCIH | GCWN | GSEC | PCIP | QSA
- Bentley University / SANS Technology Institute
- Supervisor – IT Assurance & Security
- 0xSeanG on social

# Key Terms

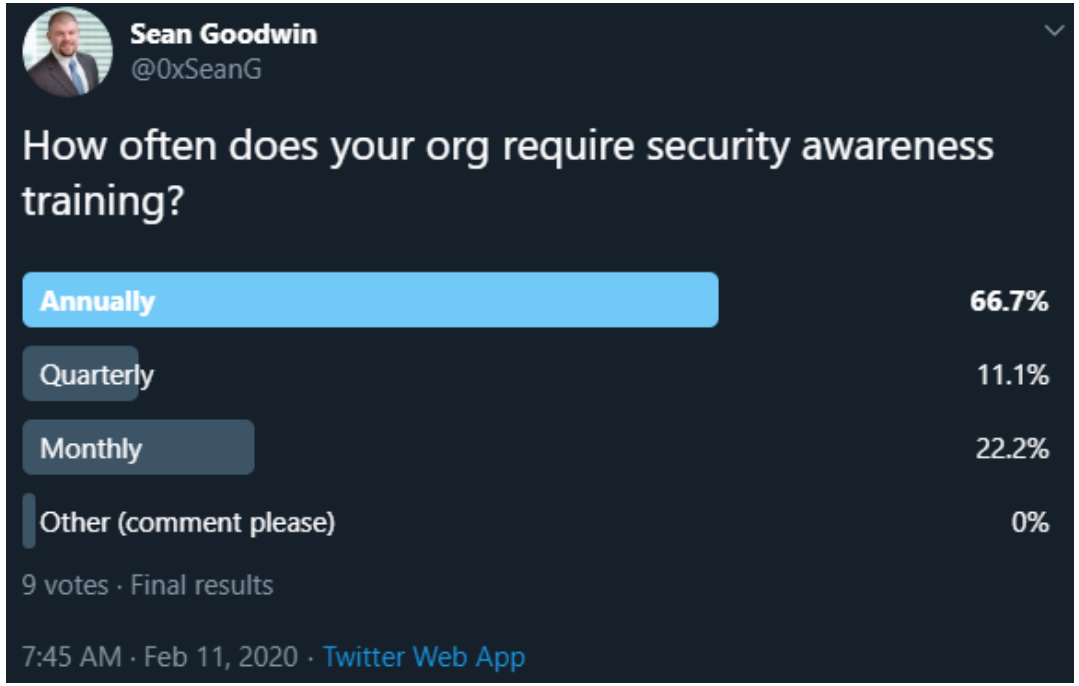
- **AWARENESS**
  - focuses on changing behaviors
- **TRAINING**
  - teaches new skills
  - will be role-specific

# That's a Compliance or HR Function

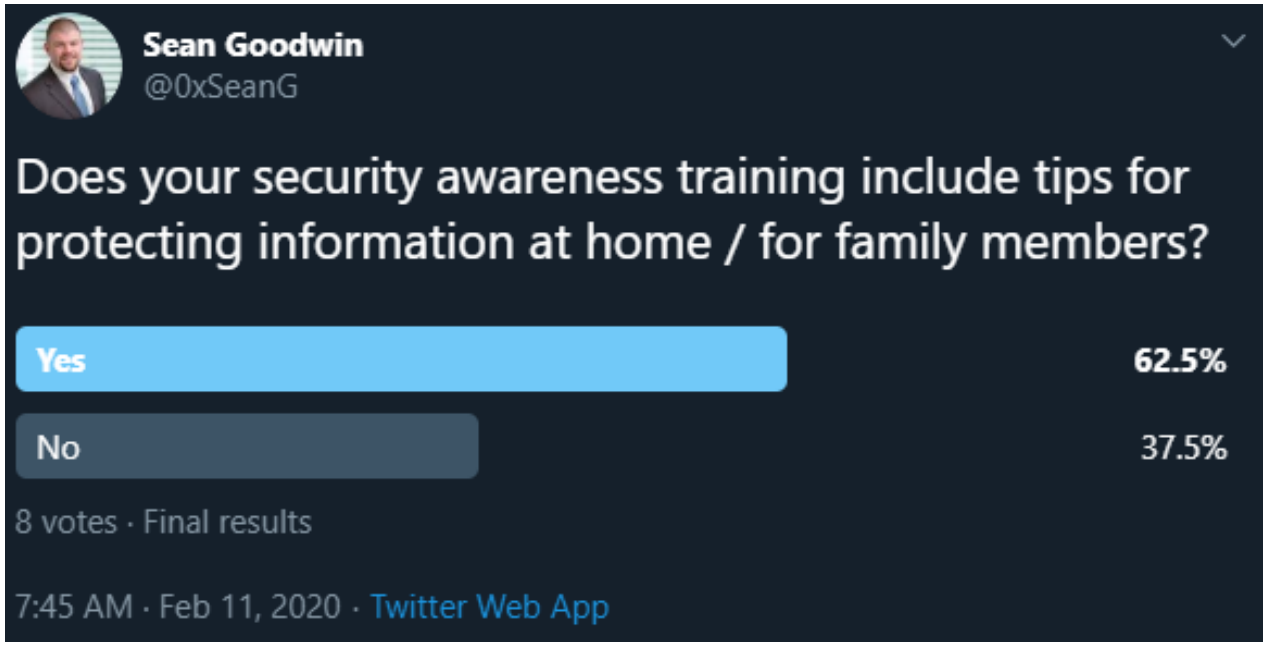
- Compliance-driven Programs
- "I think HR covers that during on-boarding"
- IT/IS too busy chasing down alerts to train users

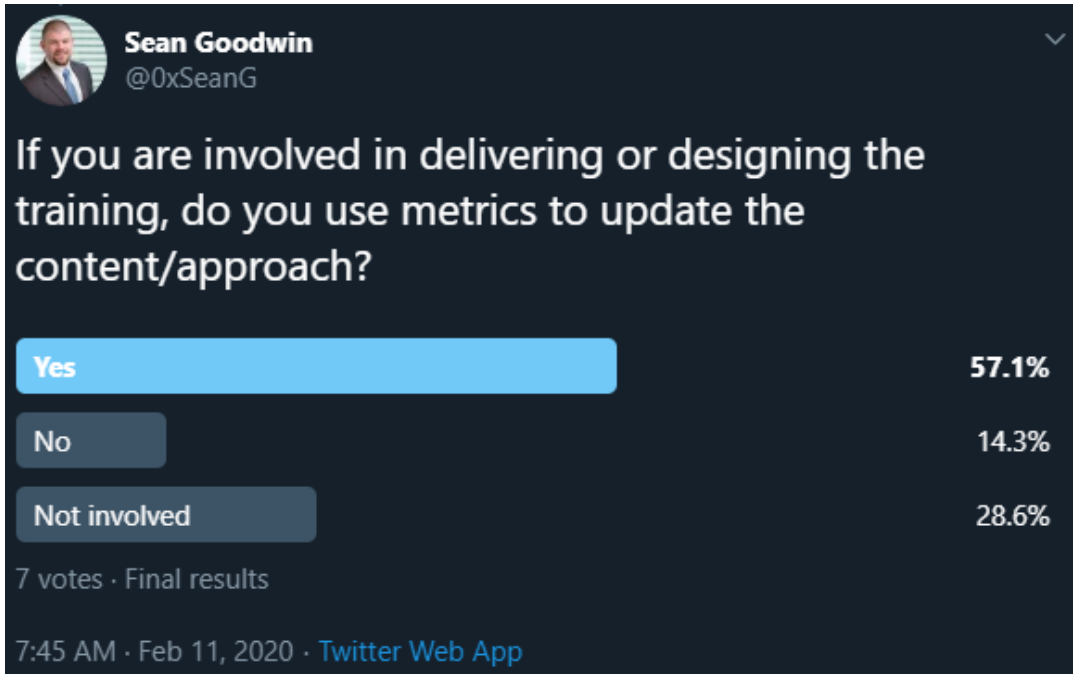


# Polling for Data

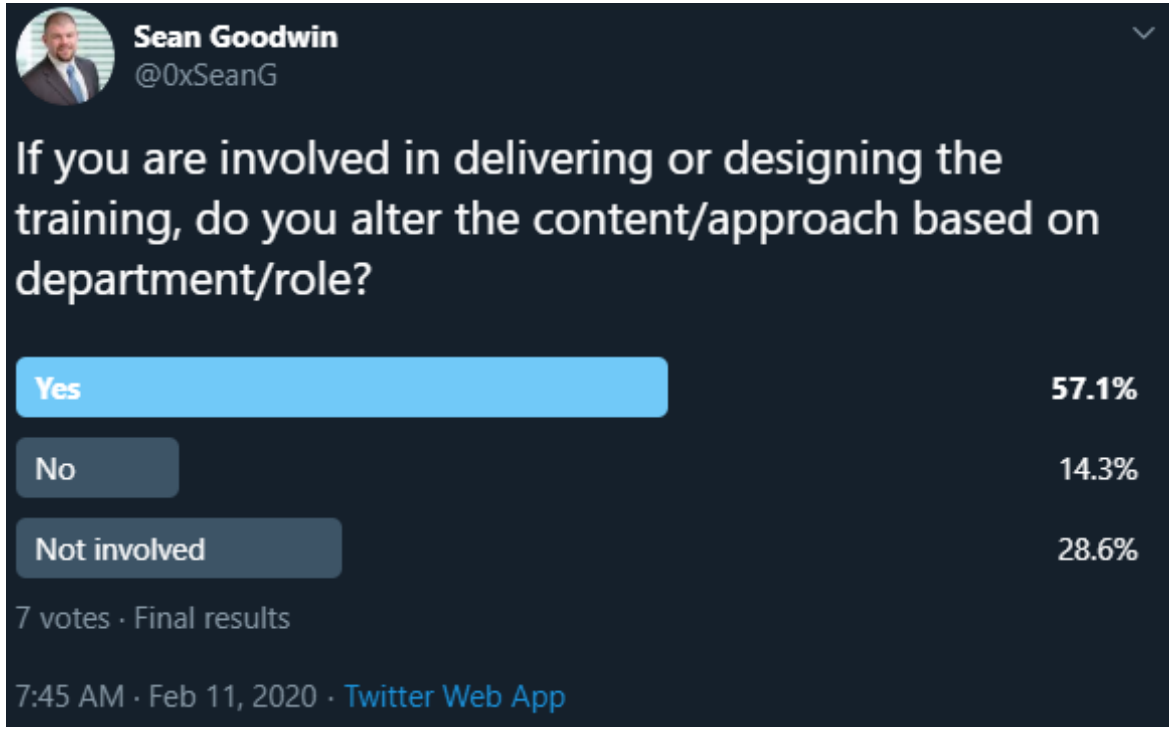



# Polling for Data



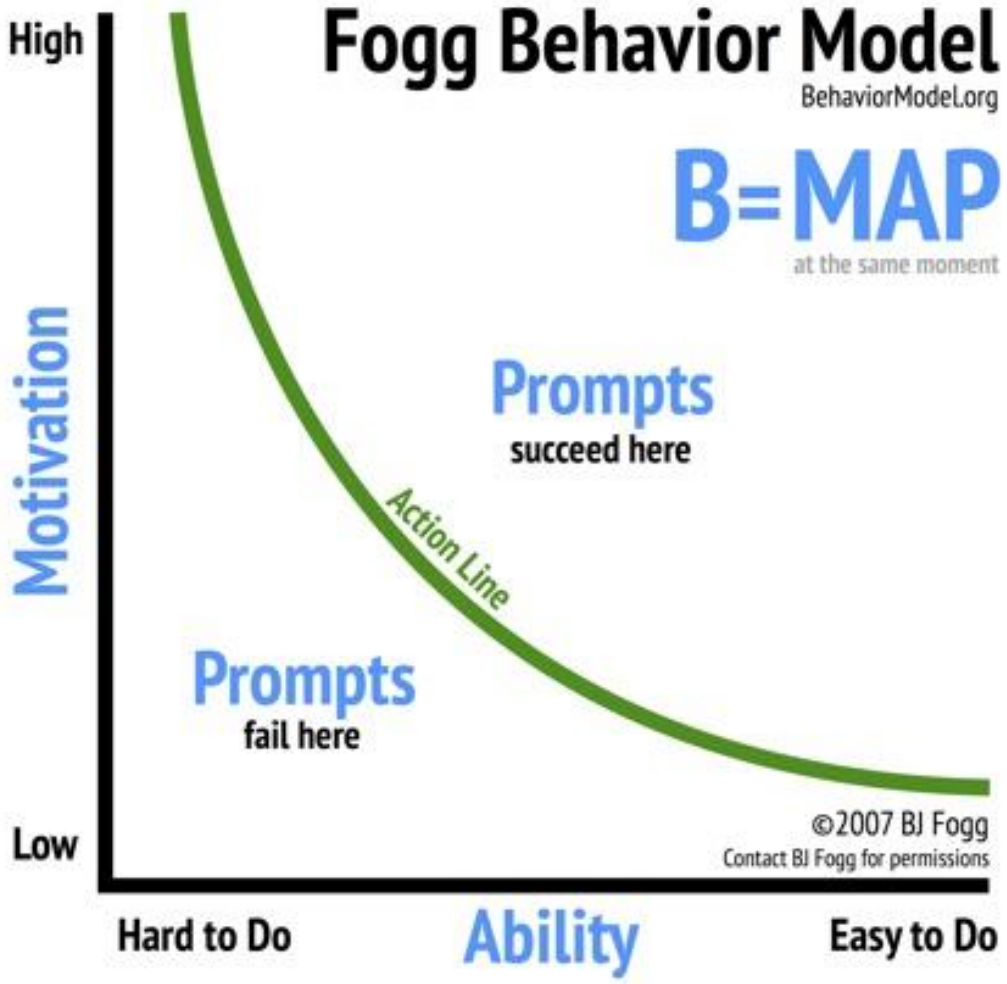



# Polling for Data




# IT/IS Misses the Mark

- “Curse of Knowledge”
- End users are too dumb
- Focuses on the wrong things




https://www.behaviormodel.org/

WOLF
& COMPANY, P.C.

“Never let a breach go to waste” – Randy Marchany

# Executive Buy-in

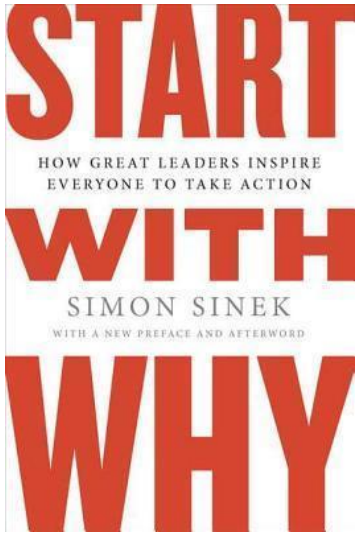
- Have a project plan in place
- Don’t go straight for the cash
- Start small
- Ditch the hoodie!!

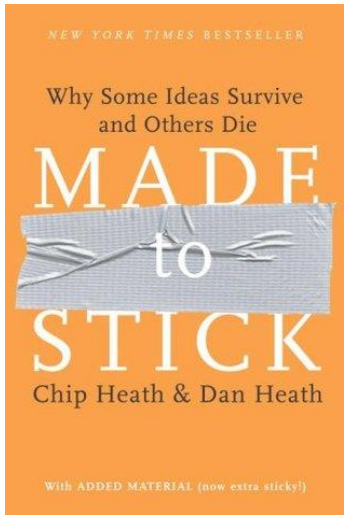

https://www.method123.com/images/project-lifecycle-v2.jpg

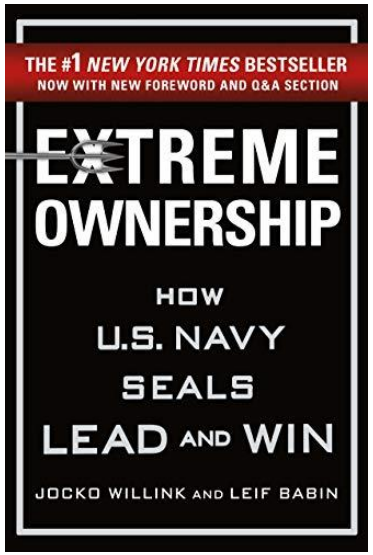
WOLF & COMPANY, P.C.

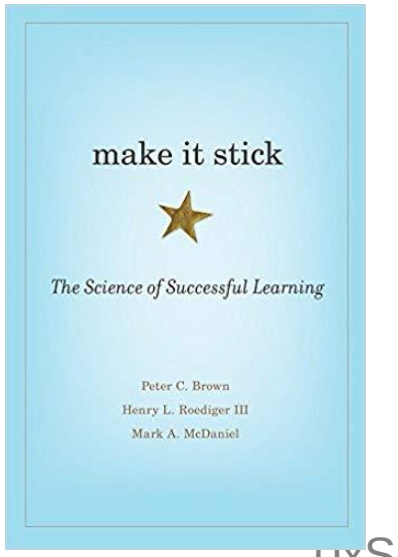
# Start with “WHY”

- Take time to understand the business
- Tailor the answer to “Why does security matter”



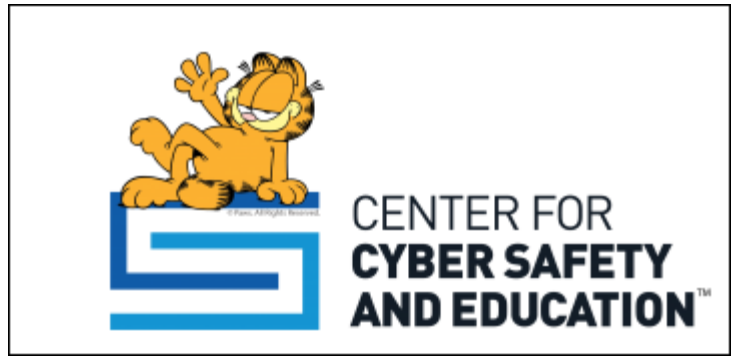
# Further Reading

- Lance Spitzner – “Top Books on Security Culture”

https://www.sans.org/security-awareness-training/blog/top-books-security-culture

# Individual Benefits

- Lunch and Learn
- Personal Device Reviews
- Resources for family members
- Special Events





# Security Awareness Committee

- Gather volunteers from all key business areas
  - Deeper understanding of their processes
  - Get someone in your corner
- Allows for easier reinforcement training sessions
  - IT/IS not always there in person
  - Themed follow-up
- Personal pride
  - Formal naming (Ambassadors, Champions, Advocates, etc.)

# POSITIVE Reinforcement

- Wall of Sheep vs. Wall of Fame
- Track “wins” by department
- Individual Kudos


https://www.wallofsheep.com/

WOLF & COMPANY, P.C.

# Final Points

- Keep it short / non-technical
- Provide updates to leadership
- Play the long game
- Focus on small “wins”

WOLF & COMPANY, P.C.

# Resources

https://seangoodwin.blog/**wwhf-ww-2020**