ROCK the BOAT
Transforming Security Culture through Innovation

Graham J. Westbrook, C|EH, Sec+
Information Security Office

Geisinger
Traditional Security Awareness

- Target compliant ≠ target secure
- Check the box...
  - HIPAA §164.308(a)(5)
  - NIST 800-53A Rev.4 (AT-2)
- ... and then keep going...
“...What if, and I know this sounds kooky, we communicated with the employees...”
MISSION:
SECURE
Build Your Own Gamified Program

Scout the Terrain

Study the Enemy

Inspect the Crew

Chart new Course

Rock the Boat
Step 1: Scout the Terrain

- Topography
- Chokepoints
- The Perfect Storm
- Pitfalls
• No encryption
• No AV
• No patching
• Legacy OS
• Vendor remote access
• Local admin privileges always-on
• Poor authentication
• Limited aftermarket security enhancements
• Expensive Equipment
• Long Lifecycles
• Patient lives attached to these devices (IoB)
• Hacking tools extending to IoT
• Medical device source code on dark web
• Nascent regulatory efforts
• Lagging security implementations from manufacturing
• Lack of incentive to bake-in security
Step 2: Study the Enemy

• Threat-driven education
  • Adversaries?
  • Tactics?
  • Capabilities?

• Threat intelligence → curriculum
Step 3: Inspect the Crew

- Observe the cultural fabric
- Get beyond behavior management
- Remember: identity precedes activity
- Create practical hassle factor
- Co-opt status quo bias
  - reinforce secure decision-making
- Build a cultural firewall
Step 4: Chart New Course

- Identify true destination
- Choose your vessel
- Involve the officers
- Equip to win
- Fly a flag
**Step 5: Rock the Boat!**

- Be wildly creative
- Conduct bold branding/radical marketing
- Incentivize
- Employ “thrill theory”
  - Familiar objective
  - Meaningful adventure
  - Novel experience
- **Y1**: pilot
- **Y2**: larger scale, more mobile
- **Y3**: Digital deploy, at scale, min. FTE
Measure Impact and Communicate to Leadership

- Creative metrics:
  - Phish Scores (pre vs. post)
  - Phish Scores (attendees vs. non)
  - Time-to-secure
  - ‘Test’ Scores
  - Stats Y1-Y2-Y3
  - Survey Samples

- B.L.U.F. to leadership
Top Three Mistakes to Getting Started

1. Creativity-without-scale
   • Start scalable

2. Innovation isolation
   • Involve others

3. Behavior management
   • Tell a story
Methodology

1. Scout the Terrain
   identify: unique risks, storms

2. Study the Enemy
   threat Intel → curriculum

3. Inspect the Crew
   ‘do cyber better’
   identity precedes activity

4. Chart New Course
   goal: true sense of urgency

5. **Rock the Boat!**

Notes

Target compliant ≠ target secure

Rocking the Boat

≠ a purpose or a destination
≈ a map and methodology

Measuring Impact

> Metrics

...requires creativity and clarity

Mistakes

= creativity w/out scale, innovation
isolation & behavior mgmt.
Questions?