ACT Meeting – Oct 23 2019, Ft Worth, TX

10/23/19 Security Issues Breakout - Summary of Notes

Work Group Chairs - George Robertson & Scott Lindsey gave overview of work group focus and progress.

Scott Lindsey explained value of Security Issues work group

MAIN DISCUSSION: Cyber & Security Challenges

Table Discussions Questions:

1. The challenge is an urgency to be cyber-safe. What is needed to truly *DRIVE* agencies to take action?
2. In looking at the ACT Agency Cyber Guide, what format and usability changes can be made to improve usefulness and engagement?
3. What other areas of Security are needed to be addressed to help all stakeholders in our distribution channel?
4. What format for these is most effective;
   - Short, pointed articles?
   - Checklist-style priorities?
   - Links to resources?

---

1) The challenge is an urgency to be cyber-safe. What is needed to truly DRIVE agencies to take action?

- Awareness *(Must be clear and engaging)*
- Penalties & Fines
- Lawsuits
- Audits by state
- Impact to their business
  - Public knowledge/loss of data
  - First agency to make headlines
- Employee training/education
  - Poor employee practices/actions "cause" hacking
  - Must provide continual training
  - Do internal test/checks
    - Demonstrate how they can be affected/staff doesn't recognize the "importance" data has
    - Create repercussions for "failing"
  - Offer CE credit
- Create plan for agency owners to follow/implement

2) In looking at the ACT Agency Cyber Guide, what format and usability changes can be made to improve usefulness and engagement?

- Culture
  - All levels of organization need to get the message
  - Set up consequences for not meeting *(the regulations?)*
  - Work to address misconceptions and provide clarity – where do agents go?
- ACT/CIS guide
  - No one at table had clear understanding of that guide – *reveals lack of recent communication?*
- Collaborative guide or session
  - Sessions with "goal of the month" format
  - Classes and walk throughs (video walk through too)
  - Videos - quick, 5 minutes with real examples
- Break into a timeline
- Correct links
- Simplify the message/Too wordy
- Separate document with vendor info

3) What other areas of security are needed to be addressed to help all stakeholders in our distribution channel?

- Encryption
  - Agents encrypt outgoing emails but incoming are not encrypted
    - How can this be addressed?
  - All levels should be protected – not just email – consider messaging etc.
- Personally Identifiable Information (PII)
  - Need to clarify what it is and what it is <u>not</u>
- Multiple levels of protection are needed – single level puts more at risk than multi levels
- Third party security
  - Vendors
  - APIs
    - API Penetration ('Pen') testing
  - False sense of security from both
- "Right to be Forgotten" – scrubbing data
- "Map" of where data is
  - Agency management system but other apps too
  - Where else is data stored
- Procedures must be followed to allow claims to be defended

4) **What format for these is most effective:**

- **Short, pointed articles? Checklist-style priorities? Links to resources?**
  - Short articles with links **that work**
  - Videos with "You tube" like delivery
  - Working sessions
  - Conferences
  - Staff meetings in agency
  - Security Experts library
  - Certification – *potentially Big 'I'-sponsored?*

Additional Resources mentioned:

Insurashield – Westfield

- Allows small and mid-sized agents same security available to large enterprises