Miriam E. Armstrong, Keith S. Jones, & Akbar Siami Namin
Texas Tech University

Motivation
- Cybersecurity is an increasingly prevalent and expensive problem
- Future cyber professionals should be trained based on the Knowledge, Skills, and Abilities (KSAs) they’ll need once they graduate
- Research with cyber professional participants encounters four main constraints
  - No naturalistic observations
  - Anonymity and safety
  - Short data collection time
  - No deep process questions
- Traditional TA & CTA methods do not fit within the constraints; this makes participant recruitment difficult
- Need for methodology that works within the 4 constraints

This poster outlines:
- The 4 constraints to researching cyber professionals
- Accommodations for each constraint (including the brief interview technique that we used)
- The effectiveness of our methodology

Development of Brief Interview Technique
- With a subject matter expert, we identified four potential constraints to research
- We found accommodations for each constraint, thus creating the brief interview technique
- We implemented the brief interview technique to collect data and to evaluate our brief interview technique
- 44 participants at Black Hat and DEF CON
  - Interviewed independently
  - Participants could skip any questions

Brief Interview Technique:
- 5 demographic questions (e.g., years in cyber, education level)
- 64 KSAs questions
- 32 KSAs; asked 2 multiple choice questions for each
- 12 open-ended questions (e.g., “What tools do you use to perform packet level analysis?” “What soft skills are most important for your job?” “Was there anything you had to learn on the job that you wish you had learned at school?”)

Constraints

<table>
<thead>
<tr>
<th>Limitations to research involving cyber professionals</th>
<th>Ways a methodology could fit within the constraints</th>
<th>How well our interview technique fit within the constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Naturalistic Observations</td>
<td>Individual interviews rather than naturalistic observation</td>
<td>n/a (we did not attempt to collect observation data)</td>
</tr>
<tr>
<td>• Need to keep information secure</td>
<td>• Alternative accommodation:</td>
<td></td>
</tr>
<tr>
<td>• Need to keep specificities of work process secure</td>
<td>• observe training scenarios</td>
<td></td>
</tr>
<tr>
<td>• Vulnerabilities may be exposed through publishing research findings</td>
<td>(close approximation of real cyber work)</td>
<td></td>
</tr>
<tr>
<td>• May need to recruit all team members</td>
<td>For large, diverse participant pool:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• In-person interviews; no online data collection</td>
<td></td>
</tr>
<tr>
<td>Anonymity and Safety</td>
<td>• Notes taken on paper; no video or audio recordings</td>
<td></td>
</tr>
<tr>
<td>• Need to protect employer and self</td>
<td>• No demographic questions concerning gender or</td>
<td></td>
</tr>
<tr>
<td>• Internet surveys may not be considered safe</td>
<td>• race (education, years in cyber ok)</td>
<td></td>
</tr>
<tr>
<td>• When recruiting from large, diverse participant pools:</td>
<td>• No names; no participant compensation</td>
<td></td>
</tr>
<tr>
<td>• Name and workplace may be sensitive information</td>
<td>• For small participant pools, most accommodations</td>
<td></td>
</tr>
<tr>
<td>(this poses problems for participant compensation)</td>
<td>would be the same as above except participant</td>
<td>would likely be necessary</td>
</tr>
<tr>
<td></td>
<td>compensation would likely be necessary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To protect personal information would be collected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Participants did not skip demographic questions</td>
<td></td>
</tr>
</tbody>
</table>

Short Data Collection Time
- Cyber professionals are expensive, busy
- Limit interview to 15 minutes
- Our interview ran long; some participants left early

No Deep Process Questions
- Need to keep information secure
- Need to keep specificities of work process secure
- Vulnerabilities may be exposed through publishing research findings
- Ratings scale on importance of KSAs in cyber work (taken from NICE Framework)
- Which tools do you use for x task?
- Open-ended questions about tools, soft skills
- No questions skipped for being too invasive
- Data was sufficient for our purposes

Limitations
- Unclear when each constraint does or does not apply
- Observations, deep process questions have been done in the past (D’Amico & Whitney, 2008; Mahoney et al., 2010)
- The brief interview technique relies on self-report; ideally data would be validated by objective measures of work performance

Conclusions
- Our brief interview technique fit within the 4 constraints
- Data collected is pertinent to development of cybersecurity education, training, and exercises
- Technique has fast turnaround time
- Technique is customizable to
  - Personnel selection
  - Other cyber-related research
  - Research of other high-security populations

References

This work is supported by the National Science Foundation under award number DGE-1551636
Poster presented at HFES 2017 at the JW Marriott, Austin, TX, USA