Framework for Developing a Brief Interview to Understand Cyber Defense Work: An Experience Report

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 KSA 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 Limitations to research involving cyber professionals	Accommodations Ways a methodology could fit within the constraints	Lessons Learned How well our interview technique fit within the constraints
No Naturalistic Observations • Need to keep information secure • Need to keep specificities of work process secure • Vulnerabilities may be exposed through publishing research findings • May need to recruit all team members	• Individual interviews rather than naturalistic observation • Alternative accommodation: • observe training scenarios (close approximation of real cyber work)	• n/a (we did not attempt to collect observation data)

Anonymity and Safety
• Need to protect employer and self
• Internet surveys may not be considered safe
• When recruiting from large, diverse participant pools:
  • Name and workplace may be sensitive information (this poses problems for participant compensation)
• When recruiting from small participants pools (e.g., when participants are recruited from only one or two organizations):
  • Demographic information may be identifying information
	• For large, diverse participant pool:
	  • In-person interviews; no online data collection
	  • Notes taken on paper; no video or audio recordings
	  • No demographic questions concerning gender or race (education, years in cyber ok)
	  • No names; no participant compensation
	• For small participant pools, most accommodations would be the same as above except participant compensation would likely be necessary
		• We recruited from a large, diverse participant pool by collecting data at large cyber conferences; recruited 44 participants in 5 days with 2 interviewers
		• Reluctance to participate until guaranteed that no personal information would be collected
		• Participants did not skip demographic questions

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

D'Amico, A., & Whitley, K. (2008). The real work of computer network defense analysts. In J. R. Goodal, G. Conti, & K. Ma (eds): *VIzSEC 2007* (pp. 19-37). Springer Berlin Heidelberg.

Mahoney, S., Roth, E., Steinke, K., Pfautz, J., Wu, C., & Farry, M. (2010). A cognitive task analysis for cyber situational awareness. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58,* 415-418.

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

This work is supported by the National Science Foundation under award number DGE-1516636
Poster presented at HFES 2017 at the JW Marriott, Austin, TX, USA