Technological Con-Artistry: An Analysis of Social Engineering

KANSAS STATE UNIVERSITY

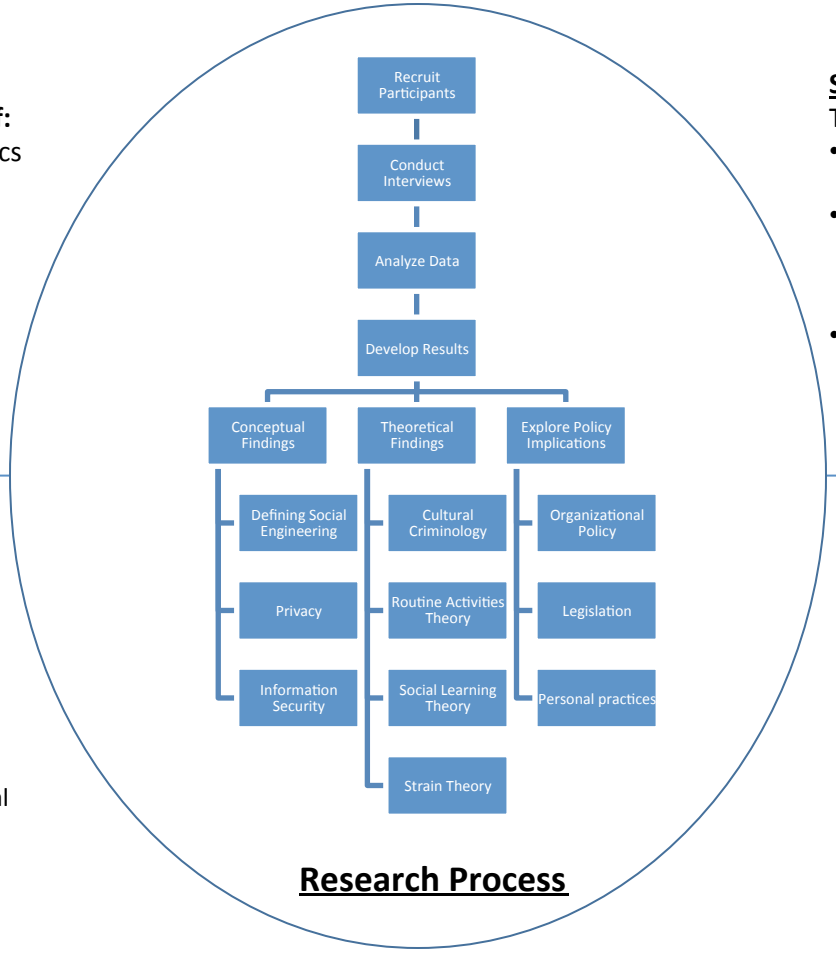
Challenge:

To develop a deeper understanding of:

- the motivations and characteristics of social engineers;
- the process by which social engineering is accomplished;
- the nature of the threat and strategies used to combat it by personnel involved in IT security.

Solution:

- A non-experimental, cross-sectional research design will be used that employs a multi-methodological approach for data collection.
- Personal interviews will be used to collect both qualitative and quantitative data.
- Interviews will be conducted with subjects drawn from three populations involved in the perpetration and prevention of social engineering: social engineers "in the wild," information security auditors, and IT professionals in charge of managing organizational data security.



Research Process

Scientific Impact:

This study will

- Be one of the first criminological studies of social engineering;
- Provide an understanding of the role of group dynamics in the creation and implementation of social engineering strategies;
- Develop a criminological theory of social engineering.

Broader Impact:

- Social engineering potentially poses a threat to anyone requiring IT security;
- Will provide a clearer picture of the real threat social engineering poses to IT security;
- Can inform the policies of government and business organizations regarding information security;
- Will produce findings that will be used to educate and inform students of criminology.

#SES-1616804, Kansas State University, Kevin Steinmetz PI (785 532-4974)(kfsteinmetz@k-state.edu); W. Richard Goe Co-PI (785 532-4973)(goe@k-state.edu)