Workshop ID: F6
Title:
Reconsidering assumptions about the human role in cybersecurity and privacy research

1) Short Description

In cyber security research, the role of "human" is often discussed with a negative undertone, framing employees as 'insider threats', 'computer abusers', or 'cyber deviants' when they do not comply with the prescribed security rules. Whether the negative perspective is a paradigm (Morgan, 1980) can be discussed, but there are certain prevalent metaphors such as the human being "the weakest link" in the information security chain. Using criminological theories, such as deterrence and neutralization theory, persuades us to accept the assumption that a non-compliant employee is performing a "white collar crime" (Straub & Nance, 1990, p. 46). Further, to Morgan's (1980) classification, suggesting intimidating employees into compliance with punishment and fear appeals has become a de facto puzzle-solving (i.e. specific solutions to specific problems) practice.
What if, when discussing puzzle-solving solutions, we would discuss incentives instead of sanctions? On the metaphor level, what if we researchers challenged the negative assumptions behind deterrence, neutralization, and protection motivation theories and replaced them with self-determination theory or socio-technical approaches? Self-determination theory by Deci and Ryan (1980) argues that people have an intrinsic need for autonomy, competence, and relatedness. This triad could translate to inspiring aspects such as empowering with knowledge, the joy of gamifying, and a sense of community.
Or if we use some other metaphors such as Johnston et al. (2019) "It takes a village" or the idea of security as a team sport (Yoo et al., 2020) or 'human-as-solution'(Zimmermann & Renaud, 2019)? We would view humans as valuable actors, and first responders to security threats. This kind of imagery is needed for the empowerment of humans as an integral part of an information security management system.
We invite papers problematizing the negative assumptions and solutions, or even the way of seeing the reality in cyber security as well as privacy research, whether they employ qualitative, quantitative, conceptual, or other research approaches.

---

2) Detailed Description

In cyber security research, the role of "human" is often discussed with a negative undertone, framing employees as 'insider threats', 'computer abusers', or 'cyber deviants' when they do not comply with the prescribed security rules. Whether the negative perspective is a paradigm (Morgan, 1980) can be discussed, but there are certain prevalent metaphors such as the human being "the weakest link" in the information security chain. Using criminological theories, such as deterrence and neutralization theory, persuades us to accept the assumption that a non-compliant employee is performing a "white collar crime" (Straub, 1989, p.154). Further, to Morgan's (1980) classification, suggesting intimidating employees into compliance with punishment and fear appeals has become a de facto puzzle-solving (i.e. specific solutions to specific problems) practice.

What if, when discussing puzzle-solving solutions, we would discuss incentives instead of sanctions? On the metaphor level, what if we researchers challenged the negative assumptions behind deterrence, neutralization, and protection motivation theories and replaced them with self-determination theory or socio-technical approaches? Self-determination theory by Deci and Ryan (1980) argues that people have an intrinsic need for autonomy, competence, and relatedness. This triad could translate to inspiring aspects such as empowering with knowledge, the joy of gamifying, and a sense of community.
Or if we use some other metaphors such as Johnston et al. (2019) "It takes a village" or the idea of security as a team sport (Yoo et al., 2020) or 'human-as-solution'(Zimmermann & Renaud, 2019)? We would view humans as valuable actors, and first responders to security threats. This kind of imagery is needed for the empowerment of humans as an integral part of an information security management system.
We invite papers problematizing the negative assumptions and solutions, or even the way of seeing the reality in cyber security as well as privacy research, whether they employ qualitative, quantitative, conceptual, or other research approaches
Interesting topics include (but are not limited to):

- *Problematizing current imagery of the human role in security and privacy*
- *Intrinsic and extrinsic motivation to improve security and privacy behavior*
- *Community and team approach to improve security and privacy behavior*
- *Gamification in security and privacy*
- *Empowering humans in security and privacy*
- *AI in cybersecurity and privacy*

Workshop format (max. 750 characters)
Format: We invite short abstracts (max 500 words) and extended abstracts (max 5000 words) to this paper development workshop. We welcome both papers in early phase from authors who wish to expose their ideas for discussion and more well-developed manuscripts from authors who wish to present and discuss their arguments before submission to a journal.
All accepted submissions will be shortly presented to the audience ("pitch talks") and then discussed in roundtable sessions so that more discussion time is allocated to extended abstracts.
Planned duration (i.e., half or full day)
Duration: 1-day workshop
Preliminary schedule:

- *09:00 Registration and morning coffee*
- *9:15 Welcome speech*
- *09:30 Workshop starts*
- *09:30 Keynote 1*
- *10:30 Break*
- *10:45 Paper presentations 1*
- *11:30 Lunch*
- *12:30 Roundtable Session 1*
- *14:00 Panel discussion or Keynote 2*
- *(15:00 Paper presentations 2*
- *15:45 Roundtable session 2)*
- *17:15 Workshop ends*

The schedule depends on the number of submissions we will receive. That is, the second paper presentation and roundtable session will be removed from the schedule if there are not enough papers to discuss.
Target audience and expected attendance

We expect IS scholars interested in cybersecurity (/IS security) and privacy to be potential participants. ECIS does not have a dedicated security & privacy track so this workshop could provide a platform for those discussions. Based on our prior experience, we expect to have between 15-30 participants.
Workshop program committee members (if applicable)
The organizers intend to use peer review for all submissions. Others who have submitted their work to the workshop will need to agree to serve as peer reviewers. The workshop is planned to be inclusive. We aim to accept all submissions that fit the scope of the workshop.
Workshop participation application deadlines
Submission deadline: April 30, 2024
Peer feedback deadline: May 21, 2024
These dates are not final but approximations. We will define the exacts dates once we know when the ECIS early-bird registration period ends. Optimally, we would like the authors to get feedback before the end of early bird to enable them to register with lower fee.

---

3) Organizers (Workshop Chairs):

Jonna Järveläinen, jonna.k.jarvelainen@jyu.fi (Contact person)
Wael Soliman, wael.soliman@uia.no
Paolo Spagnoletti, pspagnoletti@luiss.it
Marko Niemimaa, marko.niemimaa@uia.no
João Baptista, j.baptista@lancaster.as.uk
Shuyuan Metcalfe, smho@fsu.edu

---

4) Submission link\site\email

ecis2024-sigsec@jyu.fi